Guilherme Saraiva Carlos

Pontos Racionais em Circunferências

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Junho 2016

Guilherme Saraiva Carlos

Pontos Racionais em Circunferências

Tese submetida à Faculdade de Ciências da Universidade do Porto para obtenção do grau de Mestre em Matemática

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Junho 2016

Resumo

O algoritmo de Aubry é um procedimento que permite obter soluções inteiras das equações de circunferências da forma $x^2 + y^2 = n$, para alguns $n \in \mathbb{N}$, a partir de soluções racionais. Este algoritmo permite estabelecer uma correspondência entre os pontos racionais dessas circunferências com as decomposições de n em somas de dois quadrados.
Dois pontos da circunferência que correspondem à mesma decomposição dizem-se pertencer à mesma classe Aubry. Formalizando a noção natural de medida dessas classes, foram criados testes computacionais para tentar estimar as suas medidas.
Os testes foram aplicados em circunferências com exactamente duas classes de Aubry, tendo os resultados mostrado que nenhum dos testes analisados é fidedigno para estimar as medidas dessas classes, o que não deixa de ser interessante, pois é um resultado em si mesmo bastante misterioso.

Palavras Chave: Algoritmo de Aubry, Pontos Racionais em Circunferências, Somas de Dois Quadrados, Classes de Aubry.

Conteúdo

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

Este trabalho envolve um algoritmo desenvolvido em 1912 por M. Léon Aubry [7, pp. 292–295]. O algoritmo consiste em encontrar soluções inteiras da equação da circunferência $x^2 + y^2 = n$, com $n \in \mathbb{N}$ fixo, a partir de soluções racionais. Mais precisamente, o algoritmo parte de um dado ponto de coordenadas racionais e, considerando a recta que passa por esse ponto e pelo ponto de coordenadas inteiras que lhe é mais próximo, verifica-se que esta recta intersecta a circunferência num outro ponto de coordenadas racionais. Acontece que os denominadores das coordenadas do novo ponto da circunferência são menores que os das coordenadas do ponto dado. Se o novo ponto não tiver coordenadas inteiras, considerando de novo a recta que passa por este ponto e pelo ponto de coordenadas inteiras que lhe é mais próximo, obtém-se um outro ponto de coordenadas racionais da circunferência com denominadores ainda menores. Repetindo este processo, o algoritmo retorna mais tarde ou mais cedo um ponto de coordenadas inteiras dessa mesma circunferência. Portanto, cada ponto racional da circunferência dá origem, por este processo, a um ponto de coordenadas inteiras da mesma.

Um ponto de coordenadas inteiras da circunferência corresponde a uma decomposição de n em soma de dois quadrados. Acontece que cada um destes pontos dá origem a uma família de oito pontos, substituindo os sinais das coordenadas ou alternando as abcissas com as ordenadas, que estão associados à mesma decomposição em soma de dois quadrados. Assim, cada ponto de coordenadas racionais da circunferência corresponde, pelo método de Aubry, a uma família de pontos de coordenadas inteiras, e consequentemente, a uma decomposição em soma de dois quadrados. Portanto, podemos dividir os pontos racionais da circunferência através de classes de equivalência. Acontece que dois pontos pertencem à mesma classe se corresponderem à mesma decomposição de n em soma de dois quadrados.

Sabe-se ainda que se uma circunferência $x^2 + y^2 = n$ tiver mais que uma classe, então n é composto e, em particular, é possível explicitar uma factorização. Portanto, havendo um mecanismo que encontrasse todas as classes de pontos de coordenadas inteiras de qualquer

circunferência, seria possível encontrar factorizações de alguns números. Nesta dissertação foram desenvolvidos algoritmos computacionais, usando a ideia de Aubry, para procurarem essas classes e para verificarem as percentagens de pontos testados que pertenciam a cada uma das classes.

No capítulo 2 descrevem-se quais são os números que são decomponíveis em soma de dois quadrados. Além disso, mostra-se que os números que têm, pelo menos, duas decomposições distintas em soma de dois quadrados são compostos. Conhecendo essas decomposições de um dado número, é possível factorizar esse número.
No capítulo 3 aborda-se o algoritmo desenvolvido por Aubry, incluindo os resultados que sustentam o seu funcionamento. Estuda-se ainda as classes de pontos que este algoritmo origina.
No capítulo 4 apresentam-se testes para encontrar as classes em circunferências, bem como para se perceber qual é a percentagem de pontos que pertence a cada classe. Mostram-se alguns resultados em alguns exemplos de circunferências.

Capítulo 2

Somas de Dois Quadrados

Um dos primeiros registos sobre a decomposição de um número natural como soma de quadrados remonta ao século II e deve-se a Diofanto de Alexandria, que na sua Aritmética trata do problema de expressar um número da forma $A = 2a + 1$ como $x^2 + y^2$, satisfazendo as condições $x^2 > a$ e $y^2 > a$, com $x, y, a \in \mathbb{Q}$. Além de tratar de somas de dois quadrados, Diofanto também investigou a possibilidade de um número ser escrito como soma de três quadrados, especificamente nos casos em que esse número é da forma $A = 3a + 1$.
Séculos depois, Pierre de Fermat, analisou os resultados de Diofanto acima referidos e rapidamente observou algumas restrições módulo 4 e 8, para que um número seja decomponível em soma de dois ou três quadrados. Em particular observou que números da forma $4n + 3$ não podem ser escritos como soma de dois quadrados e que os números da forma $8n + 7$ não podem ser escritos como soma de três quadrados [7, p. 30]. Este ainda estudou sobre a soma de quatro quadrados, e afirmou que qualquer número pode ser escrito como soma de quatro quadrados inteiros [7, pp. 177–178].
No dia de Natal de 1640, Fermat enviou uma carta a Mersenne onde afirmava que qualquer primo da forma $4n + 1$ tem uma e só uma decomposição em soma de dois quadrados [7, p. 67].
Interessado nos resultados do matemático francês, Leonhard Euler demonstra todos os resultados de Fermat sobre soma de dois quadrados entre 1742 e 1749, que careciam de prova. Por fim, numa carta enviada a Christian Goldbach em 1749, Euler enuncia o resultado que descreve exactamente os números que podem ser descritos como soma de dois quadrados.
Nas sua correspondência com Goldbach, Euler refere também os números decomponíveis em somas de três e quatro quadrados, e numa carta demonstra que qualquer inteiro pode ser escrito como soma de quatro quadrados racionais. Apesar de ter provado esta última afirmação, Euler tinha a intenção de provar a de Fermat sobre a soma de quatro quadrados inteiro, mas foi só em 1770 que Lagrange consegue prová-la [7, p. 177-178].

2.1 Inteiros Gaussianos

Para estudar somas de dois quadrados, é conveniente usar uma extensão de $\mathbb{Z}$ na qual todas as soma de dois quadrados são um produto de dois elementos dessa extensão.

Definição 2.1. *Um inteiro Gaussiano é um número complexo $a+bi$, onde $a,b \in \mathbb{Z}$. A norma de $a+bi$ é $\mathrm{N}(a+bi) = a^2+b^2$. Denota-se por $\mathbb{Z}[i]$ o conjunto de todos os inteiros Gaussianos.*

Em $\mathbb{Z}[i]$, a soma de dois quadrados a^2+b^2 é igual ao produto $(a+bi)(a-bi)$, o que permite fazer um estudo aritmético das decomposições em somas de dois quadrados. Antes de ver como, é necessário recordar alguns conceitos aritméticos básicos comuns a todos os anéis comutativos unitários.

Definição 2.2. *Seja R um anel comutativo unitário e sejam $a,b \in R$. Se existir $c \in R$ tal que $b = ac$, então diz-se que a* divide *b ou que b é um* múltiplo *de a, em cujo caso se escreve $a \mid b$.*

Portanto $(a+bi) \mid (a^2+b^2)$.

Definição 2.3. *Um elemento u de um anel comutativo unitário R é uma* unidade de R *se u divide 1, isto é, se u tem um inverso multiplicativo em R. Dois elementos $a,b \in R$ são* associados em R *se existe uma unidade u de R tal que $a = bu$.*

Por exemplo, as unidades de $\mathbb{Z}[i]$ são $-1, 1, i$ e i.

Lema 2.4. *A norma N de $\mathbb{Z}[i]$ tem as seguintes propriedades:*

- $\mathrm{N}(\alpha) \geq 0$,
- $\mathrm{N}(\alpha) = 0$ *sse* $\alpha = 0$,
- $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$;

para quaisquer $\alpha, \beta \in \mathbb{Z}[i]$.

Demonstração. Como a norma de qualquer elemento é uma soma de dois quadrados, então N é uma função não-negativa. É imediato que $\mathrm{N}(\alpha) = 0$ sse $\alpha = 0$.
Como $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$, vem que

$$\mathrm{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

□

Lema 2.5. *$\mathbb{Z}[i]$ é um domínio de integridade.*

Demonstração. Resulta imediatamente de $\mathbb{Z}[i] \subseteq \mathbb{C}$. □

Definição 2.6. *Dado um domínio de integridade D, um elemento $p \in D\backslash\{0\}$ que não é uma unidade diz-se* irredutível em D *se, em cada factorização $p = ab$, a ou b é unidade.*

Definição 2.7. *Um elemento não nulo p de um anel comutativo unitário R diz-se* primo *se não for uma unidade e se, para todos $a, b \in R$, $p \mid ab \Rightarrow p \mid a \vee p \mid b$.*

Definição 2.8. *Uma* norma Euclideana *num domínio de integridade D é uma função $\tau : D\backslash\{0\} \to \mathbb{N}_0$ que satisfaz as seguintes condições, para quaisquer $a, b \in D$:*

- *Se $b \neq 0$, existem $q, r \in D$ tais que $a = bq + r$, onde $r = 0$ ou $\tau(r) < \tau(b)$, ou seja, aplica-se o Algoritmo da Divisão;*
- *Se $a, b \neq 0$, então $\tau(a) \leq \tau(ab)$. Se b não for uma unidade de D, então $\tau(a) < \tau(ab)$.*

Um domínio de integridade D é domínio Euclideano *se existir uma norma Euclideana em D.*

Se b for uma unidade, a igualdade na inequação no segundo ponto acontece, pois substituindo a por abb^{-1}, tem-se a inequação $\tau((ab)b^{-1}) \leq \tau(ab)$. Logo $\tau(a) = \tau(ab)$.

Teorema 2.9. *$\mathbb{Z}[i]$ é um domínio Euclideano.*

Demonstração. Vejamos agora que N de $\mathbb{Z}[i]$ é uma norma Euclideana. Sejam $\alpha, \beta \in \mathbb{Z}[i]$ não-nulos, então $\mathrm{N}(\beta) \geq 1$. Daqui resulta que $\mathrm{N}(\alpha) \leq \mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$. Prova-se assim a segunda condição para a norma Euclideana.

Falta provar a primeira condição, isto é, o algoritmo de divisão para N. É preciso encontrar $\eta, \mu \in \mathbb{Z}[i]$ tais que $\alpha = \beta\eta + \mu$, em que $\mu = 0$ ou $\mathrm{N}(\mu) < \mathrm{N}(\beta)$.
Seja $\alpha/\beta = r + si$, com $r, s \in \mathbb{Q}$, e sejam q_1 e q_2 os inteiros mais próximos dos números racionais r e s, respectivamente. Seja $\eta = q_1 + q_2 i$ e $\mu = \alpha - \beta\eta$. Se $\mu = 0$, então fica provado. Caso contrário, pela construção de η, sabemos que $|r - q_1| \leq \frac{1}{2}$ e $|s - q_2| \leq \frac{1}{2}$. Por conseguinte

$$\begin{aligned}\mathrm{N}\left(\frac{\alpha}{\beta} - \eta\right) &= \mathrm{N}((r + si) - (q_1 + q_2 i)) \\ &= \mathrm{N}((r - q_1) + (s - q_2)i) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}\end{aligned}$$

e assim obtém-se

$$\mathrm{N}(\mu) = \mathrm{N}(\alpha - \beta\eta) = \mathrm{N}\left(\beta\left(\frac{\alpha}{\beta} - \mu\right)\right) = \mathrm{N}(\beta)\,\mathrm{N}\left(\frac{\alpha}{\beta} - \mu\right) \leq \frac{1}{2}\,\mathrm{N}(\beta).$$

Portanto tem-se que $\mathrm{N}(\mu) < \mathrm{N}(\beta)$, como desejado. Conclui-se assim que N é uma norma Euclideana. □

Definição 2.10. *Seja $(R, +, \cdot)$ um anel e I um subconjunto não vazio de R. Diz-se que I é um* ideal *de R se:*

- $\forall x, y \in I,\ x - y \in I$;
- $\forall x \in I, \forall r \in R,\ xr, rx \in I$.

Definição 2.11. *Dado um qualquer elemento a de um anel comutativo R, o conjunto dos múltiplos de a, $(a) = \{ka : k \in R\}$, é o* ideal principal gerado por *a de R.*

Definição 2.12. *Um domínio de integridade D é um* domínio de ideais principais *(ou DIP) se todo o ideal em D é ideal principal.*

Teorema 2.13. *Qualquer domínio Euclideano é um DIP.*

Demonstração. [3, p. 368] Seja D um domínio Euclideano com norma Euclideana τ, e seja I um ideal de D. Se $I = \{0\}$, então $I = (0)$, logo é principal. Supondo que $I \neq \{0\}$, existe $b \neq 0$ em I. Escolhemos b tal que $\tau(b)$ é mínima, pois $\mathbb{N}$ é bem ordenado. Para qualquer $a \in I$, pela primeira condição da definição de norma Euclideana, existem $q, r \in D$ tais que

$$a = bq + r$$

onde $r = 0$ ou $\tau(r) < \tau(b)$. Agora tem-se que $r = a - bq$ e $a, b \in I$, logo $r \in I$, pois I é ideal. Mas $\tau(r) < \tau(b)$, o que é impossível pela minimalidade de $\tau(b)$. Daqui resulta que $r = 0$, logo $a = bq$. Como a era qualquer elemento de I, tem-se que $I = (b)$. □

Teorema 2.14. *$\mathbb{Z}[i]$ é um DIP.*

Demonstração. Como $\mathbb{Z}[i]$ é um domínio Euclideano, então é um DIP pelo teorema anterior. □

Todos os elementos de $\mathbb{Z}[i]$ têm uma factorização em irredutíveis, e veremos que essa factorização é única.

Definição 2.15. *Um domínio de integridade D é um* domínio de factorização única *(ou DFU) se satisfazer as seguintes condições:*

- *Para todo o elemento de D não nulo que não seja unidade pode ser factorizado num produto finito de irredutíveis;*
- *Se $p_1 \cdots p_r$ e $q_1 \cdots q_s$ são duas factorizações do mesmo elemento de D em irredutíveis, então $r = s$ e os elementos q_i podem ser renumerados de maneira a que p_i e q_i sejam associados.*

Falta provar que $\mathbb{Z}[i]$ é DFU. Mas antes são necessários os seguintes resultados:

Teorema 2.16. *Se D é um domínio Euclideano, então todo o elemento não nulo de D ou é uma unidade ou pode ser representado como produto finito de irredutíveis.*

Demonstração. Se o teorema fosse falso, então existiriam elementos não-unidade que não teriam uma decomposição finita como produto de (um ou mais) irredutíveis. Seja $a \in D$ um elemento nessa condição tal que $\tau(a)$ seja minimal. Então a não é irredutível, e portanto, por definição, tem uma factorização não trivial $a = bc$, em que b e c não são unidades. Mas então $\tau(b) < \tau(a)$ e $\tau(c) < \tau(a)$ e b e c não podem ter ambos factorização finita de irredutíveis, caso contrário a também teria. Isto contradiz a minimalidade de $\tau(a)$. □

Proposição 2.17. *Num DIP todos os irredutíveis são primos.*

Demonstração. Seja A um DIP e $p \in A$ irredutível. Sejam $a, b \in A$ tais que $p \mid ab$. Como A é um DIP, então existe $d \in A$ tal que $(d) = pA + aA$, que é o ideal gerado pelos múltiplos de a e pelos múltiplos de p. Como p é irredutível, os seus divisores são apenas as unidades e os seus associados, e consequentemente d é unidade ou associado de p. No segundo caso, temos que $d = pu$, em que u é unidade de A. Sabemos que $pA + aA = dA = puA$, portanto existe $x \in A$ tal que $a = pux$, concluindo-se que $p \mid a$. No primeiro caso, como d é invertível, então $dA = A$, e assim $pA + aA = (1)$. Ou seja, existem $x, y \in A$ tais que $1 = px + ay$. Mas então $b = pbx + aby$ e usando o facto de que $p \mid ab$ tem-se que $ab = pc$ para algum $c \in A$. Logo b $= p(bx + cy)$, concluindo-se que $p \mid b$. □

Corolário 2.18. *Se $p, p_1, ..., p_r$ são irredutíveis num DIP D, e $p \mid p_1 \cdots p_r$, então $p = up_i$ para algum $i \in \{1, ..., r\}$, onde u é uma unidade de D.*

Demonstração. Pela proposição anterior, p é primo, logo p divide um dos factores de $p_1 \cdots p_r$. Seja p_i tal que $p \mid p_i$. Como sabemos que p_i é irredutível, resulta que é um associado de p. □

Com estes últimos resultados, podemos então provar um resultado que mostra, em particular, que o conjunto dos inteiros Gaussianos é um domínio de factorização única.

Teorema 2.19. *Todo o domínio Euclideano é DFU.*

Demonstração. [4, p. 38] Seja D um domínio Euclideano. Pelo teoremas 2.16 e 2.17, qualquer elemento $a \neq 0$ que não é uma unidade tem pelo menos uma factorização finita de primos. Supondo que existem elementos de D com duas factorizações distintas, seja a um desses elementos com a $\tau(a)$ minimal. Então

$$a = p_1 p_2 \cdots p_r = p'_1 p'_2 \cdots p'_s,$$

para alguns $p_1, ..., p_r, p'_1, ..., p'_s$ primos em D.

Como D é também um DIP, resulta pelo corolário 2.18 que $p'_1 = up_i$ para algum i. Renomeando os p_i, se necessário, podemos assumir que $i = 1$, ou seja, $p'_1 = up_1$.

$$\frac{a}{p_i} = p_2 \cdots p_r = up'_2 \cdots p'_s.$$

Como $\tau\left(\frac{a}{p_i}\right) < \tau(a)$, resulta que $r = s$ e os p'_j podem ser renomeados de modo a que p_j e p'_j sejam associados, o que mostra o que se pretendia. □

Teorema 2.20. *$\mathbb{Z}[i]$ é DFU.*

Demonstração. Como $\mathbb{Z}[i]$ é um domínio Euclideano, então é DFU pelo teorema anterior. □

2.2 Somas de Dois Quadrados

Vejamos agora quais são os números naturais que podem ser decompostos como soma de dois quadrados. Usando congruências módulo 4, obtém-se facilmente uma restrição para que um número não seja soma de dois quadrados.

Proposição 2.21. *Seja $n \in \mathbb{N}$ tal que $n \equiv 3 \pmod 4$, então n não é uma soma de dois quadrados.*

Demonstração. Se n fosse uma soma de dois quadrados, $n = a^2 + b^2$, para alguns $a, b \in \mathbb{N}$, então ter-se-ia, reduzindo módulo 4, que $n \equiv a^2 + b^2 \pmod 4$. Mas só há dois quadrados módulo 4, pois $0^2 \equiv 2^2 \equiv 0 \pmod 4$ e $1^2 \equiv 3^2 \equiv 1 \pmod 4$. Assim $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$ e portanto $a^2 + b^2 \not\equiv 3 \pmod 4$. □

Em particular, nenhum primo congruente com 3 módulo 4 é soma de dois quadrados. Pierre de Fermat descobriu que, por outro lado, todos os primos congruentes com 1 módulo 4 são somas de dois quadrados.

Definição 2.22. *Sejam $a, b\mathbb{Z}$, diz-se que $c \in \mathbb{Z}$ é o máximo divisor comum de a e b se for o maior número inteiro tal que $c \mid a$ e $c \mid b$. Denota-se por $mdc(a, b) = c$.*

Teorema 2.23. *(Fermat) Qualquer $p \in \mathbb{N}$ primo pode ser expresso de forma única como $x^2 + y^2$ (a menos de ordem das parcelas), para alguns $x, y \in \mathbb{N}$, sse $p \equiv 1 \pmod 4$ ou $p = 2$.*

Demonstração. [2, pp. 253–254], [3, pp. 377–378] No caso de $p = 2$, tem-se $p = 1^2 + 1^2$ que é a sua única decomposição como soma de dois quadrados.

No caso de p ser ímpar, pela proposição 2.21, se p é decomponível em soma de dois quadrados, então $p = 4k + 1$ ($k \in \mathbb{N}$).

Para demonstrar a implicação recíproca, assumimos que $p \equiv 1 \pmod 4$. O grupo multiplicativo dos elementos não nulos do corpo finito $\mathbb{Z}_p$ é cíclico, e tem ordem $p-1$. Como 4 é um divisor de $p-1$, vemos que $\mathbb{Z}_p$ contém um elemento n de ordem 4. Segue assim que n^2 tem ordem 2, logo $n^2 = -1$ em $\mathbb{Z}_p$. Assim, em $\mathbb{Z}$, temos que $n^2 \equiv -1 \pmod p$, logo p divide n^2+1.
Em $\mathbb{Z}[i]$, p divide $n^2+1 = (n+i)(n-i)$. Supondo que p é irredutível em $\mathbb{Z}[i]$, então também é primo por $\mathbb{Z}[i]$ ser um DIP, logo p deveria dividir $n+i$ ou $n-i$. Se p divide $n+i$, então $n+i = p(a+bi)$ para alguns $a, b \in \mathbb{Z}$, o que implicaria que $1 = pb$, que é impossível. Analogamente se vê que $p \nmid n-i$. Logo p não é irredutível em $\mathbb{Z}[i]$.
Então temos que $p = (a+bi)(c+di)$, para alguns $a+bi$ e $c+di$ que não são unidades, com $a, b, c, d \in \mathbb{Z}$. Aplicando a norma, obtém-se $p^2 = (a^2+b^2)(c^2+d^2)$. Como

$$a^2+b^2 = (a+bi)(a-bi) \neq 1 \quad \text{e} \quad c^2+d^2 = (c+di)(c-di) \neq 1$$

e p é irredutível em $\mathbb{Z}$, tem-se que $a^2+b^2 = c^2+d^2$. Logo $p = a^2+b^2$.

Falta provar que essa representação é única.
Sejam $a, b, c, d \in \mathbb{N}$ para a decomposição de p em soma de dois quadrados. Suponha-se por redução ao absurdo, que $p = a^2+b^2 = c^2+d^2$, com $a+bi \neq c+di$ e $b+ai \neq c+di$. Segue que

$$a^2d^2 - b^2c^2 = (p-b^2)d^2 - (p-d^2)b^2 = p(d^2-b^2),$$

logo $ad \equiv bc \pmod p$ ou $ad \equiv -bc \pmod p$, e como a, b, c, d são todos menores que $\sqrt{p}$, estas congruências implicam, respectivamente que

$$ad - bc = 0 \quad \text{ou} \quad ad + bc = p. \tag{2.1}$$

Supondo que a segunda hipótese é verdadeira, e como

$$p^2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2 = p^2 + (ac-bd)^2$$

então resulta que $ac - bd = 0$.

Portanto as hipóteses (2.1) implicam que

$$ad = bc \quad \text{ou} \quad ac = bd.$$

Supondo que a primeira hipótese é verdadeira, resulta que $a \mid bc$. Como $mdc(a,b) = 1$, então $a \mid c$ ou seja $c = ka$, com $k \in \mathbb{N}$. Portanto a condição $ad = bc$ reduz-se a $d = bk$. Assim,

$$p = c^2+d^2 = k^2(a^2+b^2),$$

o que implica que $k = 1$ e conclui-se que $a = c$ e $b = d$. De forma análoga, a condição $ac = bd$ leva a que $a = d$ e $b = c$. Logo a decomposição é de facto única. □

Não são, porém, somente os primos da forma $4k+1$, com $k \in \mathbb{N}$, e o número 2 que podem ser escritos como soma de dois quadrados. Para identificar todos os números que são decomponíveis em soma de dois quadrados usaremos um resultado que não demonstramos aqui (ver [2, p. 252]).

Definição 2.24. *Seja n um inteiro positivo. Um elemento $x \in \mathbb{Z}_n$ diz-se* resíduo quadrático de n, *se existir $y \in \mathbb{Z}_p$ tal que $x \equiv y^2 \pmod{n}$.*

Teorema 2.25. *(Critério de Euler) Seja p um primo ímpar e a um inteiro não divisível por p. Então $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se a é resíduo quadrático de p. E $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ se a não for resíduo quadrático de p.*

A descrição de todos os números que são somas de dois quadrados é feita no resultado seguinte.

Teorema 2.26. *Seja n um número positivo tal que $n = q^2 m$, com $q, m \in \mathbb{N}$ e m livre de quadrados. Então n pode ser representado como soma de dois quadrados sse m não contém nenhum factor primo da forma $4k+3$. Ou seja, um inteiro positivo n pode ser representado como soma de dois quadrados sse cada um dos seus factores primos da forma $4k+3$ for uma potência de expoente par.*

Demonstração. [2, pp. 255–256] Supondo que $m = 1$, e portanto não tem nenhum factor primo da forma $4k+3$, então $n = q^2 + 0^2$.

No caso $m > 1$, supondo que n é decomponível em soma de dois quadrados tem-se que $n = q^2 m = (a^2 + b^2)$, para alguns $a, b \in \mathbb{N}$. Seja $mdc(a,b) = d$, então $a = rd$ e $b = sd$, para alguns $d, r, s \in \mathbb{N}$, logo $mdc(r,s) = 1$. Segue que

$$q^2 m = d^2(r^2 + s^2).$$

Visto que m é livre de quadrados, então $d^2 \mid q^2$.

Seja p um primo ímpar que divide m. Tem-se que

$$r^2 + s^2 = \frac{q^2}{d^2}\, m = tp,$$

para algum inteiro t, logo

$$r^2 + s^2 \equiv 0 \pmod{p}.$$

Pela condição $mdc(r,s) = 1$, sabe-se que r ou s é primo com p. Supondo que é r, então existe $r' \in \mathbb{N}$ tal que

$$rr' \equiv 1 \pmod{p}.$$

Ao multiplicar a equação $r^2 + s^2 \equiv 0 \pmod{p}$ por $(r')^2$, obtém-se

$$(sr')^2 + 1 \equiv 0 \pmod{p},$$

ou seja,

$$(sr')^2 \equiv -1 \pmod{p}.$$

Portanto -1 é resíduo quadrático de p. Pelo critério de Euler, tem-se que

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

logo $p \equiv 1 \pmod{4}$. Conclui-se assim que não existe nenhum primo da forma $4k + 3$ que divida m.

Para provar a implicação recíproca, supõe-se que m não tem nenhum factor primo da forma $4k+3$. Seja $m = p_1 p_2 \cdots p_l$ a factorização de m como um produto de primos distintos. Cada um dos primos p_i é da forma $4k + 1$, podendo p_1 ser igual a 2.

A equação

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \quad (a, b, c, d \in \mathbb{Z}) \tag{2.2}$$

mostra que o produto de dois inteiros que podem ser representados como soma de dois quadrados também é decomponível como soma de quadrados. Como todos os primos que dividem p podem ser representados como soma de dois quadrados, existem x e y tal que $m = x^2 + y^2$.

Mas então

$$n = r^2 m = r^2(x^2 + y^2) = (rx)^2 + (ry)^2.$$

□

2.3 Decomposições em Duas Somas de Quadrados

Concentremo-nos agora nos números que têm exactamente duas decomposições como soma de dois quadrados. Na prova do teorema anterior, observa-se que a igualdade (2.2) prova o seguinte:

Proposição 2.27. *Sejam $a, b \in \mathbb{Z}$ decomponíveis como soma de dois quadrados, então ab também é decomponível como soma de dois quadrados.*

Ao contrário dos números primos da forma $4k + 1$, os números compostos podem ter eventualmente mais que uma decomposição como soma de dois quadrados. Por exemplo, $65 = 1^2 + 8^2 = 4^2 + 7^2$. Reciprocamente, um número que admita mais do que uma decomposição como soma de dois quadrados é necessariamente composto.

Teorema 2.28. *Seja $n \in \mathbb{N}$ tal que $n = a^2 + b^2 = c^2 + d^2$, com $(a,b),(c,d) \in \mathbb{N}^2$ e $(a,b) \neq (c,d) \neq (b,a)$. Então $n = xy$ para alguns $x, y \in \mathbb{N}$, com $x > 1$ e $y > 1$ e ambos decomponíveis em soma de dois quadrados.*

Demonstração. [5, pp. 60–62] Pela proposição 2.21 resulta que $n \not\equiv 3 \pmod 4$.

Se n é par, então $a \equiv b \pmod 2$ e $c \equiv d \pmod 2$. Observe-se que não se pode ter $a \equiv b \equiv 0 \pmod 2$ e $c \equiv d \equiv 1 \pmod 2$ (nem o recíproco), pois isto implicaria que $0 \equiv a^2 + b^2 \equiv c^2 + d^2 \equiv 2 \pmod 4$. Portanto $a \equiv b \equiv c \equiv d \pmod 2$.

Se n for ímpar, então em qualquer das suas representações como soma de dois quadrados, um dos quadrados é par e o outro é impar. Assim, em ambos os casos, pode ser assumido que $a \equiv c \pmod 2$ e $b \equiv d \pmod 2$.

Agora,

$$a^2 + b^2 = c^2 + d^2 \Leftrightarrow a^2 - c^2 = d^2 - b^2 \Leftrightarrow (a-c)(a+c) = (d-b)(d+b).$$

Seja $mdc(a-c, d-b) = k$, com $k \in \mathbb{N}$. Então $a - c = kl$ e $d - b = km$, onde $l, m \in \mathbb{N}$ são tais que $mdc(l,m) = 1$. Como $a - c$ e $d - b$ são pares, então k também é par.
Agora

$$(a-c)(a+c) = (d-b)(d+b) \Leftrightarrow kl(a+c) = km(d+b) \Leftrightarrow l(a+c) = m(d+b).$$

Como $mdc(l,m) = 1$ então $a + c = mr$ e $d + b = lr$, para algum $r \in \mathbb{N}$, e verifica-se que r é par pois $a + c$ e $b + d$ também o são.

Assim,

$$\begin{aligned} n &= \frac{a^2 + b^2 + c^2 + d^2}{2} \\ &= \frac{1}{4}((a-c)^2 + (a+c)^2 + (d-b)^2 + (d+b)^2) \\ &= \frac{1}{4}((kl)^2 + (km)^2 + (mr)^2 + (lr)^2) \\ &= \frac{1}{4}(k^2 + r^2)(l^2 + m^2) = \left[\left(\frac{k}{2}\right)^2 + \left(\frac{r}{2}\right)^2\right](l^2 + m^2). \end{aligned}$$

Como k e r são pares, então conclui-se que n é produto de dois inteiros, em que cada um é decomponível em soma de dois quadrados. □

A implicação recíproca não é verdadeira, ou seja, se n for um produto de dois números decomponíveis em soma de dois quadrados, então n pode não ter duas decomposições distintas em soma de dois quadrados.

Uma maneira de encontrar contra-exemplos é a seguinte. Suponha-se que $n = ab$, para alguns $a, b \in \mathbb{N}$ tais que $a = x^2 + y^2$ e $b = z^2 + w^2$, com $x, y, z, w \in \mathbb{N}$. Tem-se que

$$n = ab = (x^2 + y^2)(z^2 + w^2)$$

e como

$$(x^2 + y^2)(z^2 + w^2) = (x + yi)(x - yi)(z + wi)(z - wi)$$

segue que

$$\begin{aligned} n &= [(x + yi)(z + wi)]\,[(x - yi)(z - wi)] \\ &= [(xz - yw) + (yz + xw)i]\,[(xz - yw) - (yz + xw)i] \\ &= (xz - yw)^2 + (yz + xw)^2 \end{aligned} \tag{2.3}$$

e

$$\begin{aligned} n &= [(x + yi)(z - wi)]\,[(x - yi)(z + wi)] \\ &= [(xz + yw) - (xw - yz)i]\,[(xz + yw) + (xw - yz)i] \\ &= (xz + yw)^2 + (xw - yz)^2. \end{aligned} \tag{2.4}$$

Procuraremos agora $x, y, z, w \in \mathbb{N}$ tais que estas decomposições sejam as mesmas, ou seja, tais que

$$|xz - yw| = |xz + yw| \text{ ou } |xz - yw| = |xw - yz|. \tag{2.5}$$

Supondo por exemplo que $x = 0$, tem-se $|-yw| = |yw|$ na primeira igualdade. Por exemplo, sejam $a = 2^2 + 0^2$ e $b = 1^2 + 2^2$, então $ab = 20 = 2^2 + 4^2$ só tem uma representação em soma de dois quadrados.

Outros contra-exemplos são obtidos quado um dos factores for uma soma de dois quadrados iguais, isto é, se por exemplo, $a = 2x^2$. Ou seja, supondo que $x = y$, as duas igualdades (2.5) são verdadeiras e assim $|x(z - w)| = |x(w - z)|$. Como exemplo tem-se $a = 2^2 + 2^2$ e $b = 1^2 + 2^2$, em que $ab = 40 = 2^2 + 6^2$ só tem uma representação como soma de dois quadrados.

Conclui-se assim que o produto de dois números decomponíveis como soma de dois quadrados nem sempre tem mais que uma decomposição.

Neste trabalho daremos, mais à frente, particular atenção aos números da forma $n = pq$ com p, q primos distintos tais que $p \equiv q \equiv 1 \pmod 4$, números estes que têm exactamente duas decomposições distintas como somas de dois quadrados.

Proposição 2.29. *Seja $n = pq$ tal que p, q são primos distintos e da forma $4k + 1$, então n tem exactamente duas decomposições distintas em soma de dois quadrados.*

Demonstração. Sejam $p = p_1^2 + p_2^2$ e $q = q_1^2 + q_2^2$, com $p_1, p_2, q_1, q_2 \in \mathbb{N}$. Sabe-se que estas decomposições são únicas, pelo teorema 2.23. Além disso, como p e q são ímpares, então p_1 e p_2 têm paridades diferentes, bem como q_1 e q_2. Para que pq tenha somente uma decomposição em soma de dois quadrados é necessário que $|p_1q_1 + p_2q_2| = |p_1q_1 - p_2q_2|$ ou $|p_1q_1 + p_2q_2| = |p_1q_2 - p_2q_1|$.

Na primeira hipótese, se $p_1q_1 + p_2q_2 = p_1q_1 - p_2q_2$ então

$$2p_2q_2 = 0 \Leftrightarrow p_2 = 0 \vee q_2 = 0,$$

o que é impossível, pois isso implicaria que p ou q fosse um número composto.

Ainda na primeira hipótese, se $p_1q_1 + p_2q_2 = -p_1q_1 + p_2q_2$ então

$$2p_1q_1 = 0 \Leftrightarrow p_1 = 0 \vee q_1 = 0$$

que também é impossível.

Em relação à segunda hipótese, se $p_1q_1 + p_2q_2 = p_1q_2 - p_2q_1$ então

$$p_1(q_1 - q_2) = -p_2(q_1 + q_2).$$

Reduzindo módulo 2, tem-se

$$p_1(q_1 - q_2) \equiv p_1(q_1 + q_2) \equiv p_2(q_1 + q_2) \equiv -p_2(q_1 + q_2) \pmod 2,$$

e como q é ímpar então $q_1 + q_2 \equiv 1 \pmod 2$, e assim segue que

$$p_1 \equiv p_2 \pmod 2,$$

o que é absurdo, pois p é ímpar e assim ambos os quadrados que o decompõem têm paridades diferentes.

De maneira análoga, na segunda hipótese, se $p_1q_1 + p_2q_2 = -p_1q_2 + p_2q_1$ tem-se que

$$p_1(q_1 + q_2) \equiv p_2(q_1 + q_2) \equiv p_2(q_1 - q_2) \pmod 2,$$

e agora

$$p_1 \equiv p_2 \pmod 2,$$

que também é impossível.

Portanto as duas decomposições

$$(p_1q_1 - p_2q_2)^2 + (p_2q_1 + p_1q_2)^2 \quad \text{e} \quad (p_1q_1 + p_2q_2)^2 + (p_2q_1 - p_1q_2)^2 \tag{2.6}$$

são sempre distintas. Logo $n = pq$ tem sempre, no mínimo, duas decomposições distintas como soma de dois quadrados.
Trabalhando em $\mathbb{Z}[i]$, tem-se que

$$n = pq = (p_1 + p_2i)(p_1 - p_2i)(q_1 + q_2i)(q_1 - q_2i). \tag{2.7}$$

Como $\mathbb{Z}[i]$ é DFU, então os seus elementos têm uma factorização única, a menos de factores associados. Como p e q são irredutíveis em $\mathbb{N}$, então os seus factores são irredutíveis em $\mathbb{Z}[i]$. Suponhamos que existe uma terceira decomposição em soma de dois quadrados

$$n = r_1^2 + r_2^2 = (r_1 + r_2i)(r_1 - r_2i), \tag{2.8}$$

com r_1 e r_2 não nulos. Então como os elementos irredutíveis em $\mathbb{Z}[i]$ são primos, os factores de p e q dividem um dos dois factores desta decomposição.

Se $r_1 + r_2i$ tiver exactamente dois dos factores irredutíveis de n (assim $r_1 - r_2i$ tem os dois restantes), então caso o produto desses factores seja um produto de conjugados, tem-se que $r_2 = 0$, o que é absurdo. Caso contrário, a decomposição $r_1^2 + r_2^2$ será igual a uma das já conhecidas (2.6).

Por outro lado, se $r_1 + r_2i$ tem apenas um factor irredutível de n e $r_1 - r_2i$ tem os outros três, ou vice-versa, um dos factores de (2.8) é igual ou associado a um dos factores irredutíveis de n. Isto implicaria que $n = p$ ou $n = q$, o que é impossível.

Logo não existe uma terceira decomposição distinta das duas mencionadas acima. □

Capítulo 3

Algoritmo de Aubry

3.1 Dos racionais para os inteiros

Ao lidar com números cada vez maiores, torna-se cada vez mais moroso identificar quais são decomponíveis como soma de dois quadrados. Devido à dificuldade em factorizar esses números num produto de primos, determinar uma sua decomposição em soma de dois quadrados também se torna complicado. No entanto, o matemático M. Léon Aubry descobriu um algoritmo que determina uma decomposição em soma de dois quadrados inteiros de um número se se conhecer uma sua decomposição como soma de dois quadrados racionais [7, pp. 292–295].

O método de Aubry consiste em obter um ponto de coordenadas inteiras numa circunferência centrada em zero de raio $\sqrt{n}$, com $n \in \mathbb{N}$, a partir de um ponto com coordenadas racionais dessa mesma circunferência. Este algoritmo é baseado no facto de que a recta que passa num ponto P de coordenadas racionais dessa circunferência e no ponto de coordenadas inteiras que lhe é mais próximo intersecta essa mesma circunferência num segundo ponto P'. Este ponto também tem coordenadas racionais, mas com denominadores inferiores aos do ponto P. Aplicando este procedimento a P', obtém-se um terceiro ponto P'' que tem denominadores menores que P'. Iterando este processo sucessivamente com os pontos obtidos, atinge-se mais tarde ou mais cedo um ponto de coordenadas inteiras. A figura 3.1 ilustra este procedimento, onde R_i é o ponto de coordenadas inteiras mais próximo de S_i, com $i \in \{0, ..., 3\}$. Note-se que $S_3 = R_3$.

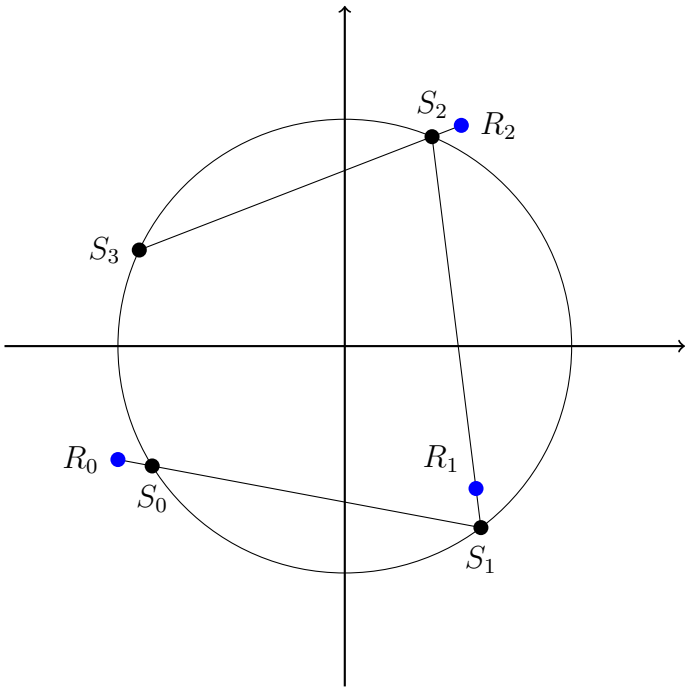

Figura 3.1: Representação Geométrica do Algoritmo de Aubry

Seja n um qualquer número que é soma de dois quadrados inteiros e seja

$$\mathcal{C}_n = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = n\},$$

onde $n \in \mathbb{N}$, o conjunto dos pontos da circunferência de raio $\sqrt{n}$ centrada na origem. O algoritmo de Aubry aplica-se no subconjunto

$$\mathcal{Q}_n = \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = n\} = \mathcal{C}_n \cap \mathbb{Q}^2.$$

Comecemos por observar que os pontos de $\mathcal{Q}_n$ têm coordenadas que, quando expressas por fracções irredutíveis, têm igual denominador.

Proposição 3.1. *Sejam $n \in \mathbb{N}$ e $\left(\frac{a}{b}, \frac{c}{d}\right) \in \mathcal{Q}_n$, com $a, c \in \mathbb{Z}$ e $b, d \in \mathbb{N}$ tais que $mdc(a, b) = mdc(c, d) = 1$. Então $b = d$.*

Demonstração. Como $\left(\frac{a}{b}, \frac{c}{d}\right) \in \mathcal{Q}_n$, tem-se que

$$n = \frac{a^2}{b^2} + \frac{c^2}{d^2} = \frac{a^2d^2 + b^2c^2}{b^2d^2}$$

e portanto

$$a^2d^2 + b^2c^2 = b^2d^2n.$$

Daqui resulta que $b^2 \mid a^2d^2$. Dado que $mdc(a, b) = 1$, vem que $b^2 \mid d^2$, concluindo-se que $b \mid d$. Analogamente, de $d^2 \mid b^2c^2$ e $mdc(c, d) = 1$, conclui-se que $d \mid b$. Como $b, d \in \mathbb{N}$ resulta que $b = d$. □

Como os denominadores são iguais em ambas as coordenadas, o respectivo número será então referido como *o denominador* do ponto dado.

Definição 3.2. *Se* $S = \left(\frac{a}{b}, \frac{c}{b}\right) \in \mathcal{Q}_n$, *com* $a, c \in \mathbb{Z}$, $b \in \mathbb{N}$ *e* $mdc(a, b) = mdc(a, c) = 1$, *diremos que* b *é o* denominador *de* S.

Além dos pontos de $\mathcal{Q}_n$ terem o mesmo denominador, existem algumas restrições quanto aos possiveis denominadores desses pontos. Em particular, 2 não ocorre como denominador.

Proposição 3.3. *Nenhum ponto de* $\mathcal{Q}_n$ *tem denominador 2.*

Demonstração. Supondo que $\mathcal{Q}_n$ tem um ponto da forma $\left(\frac{a}{2}, \frac{b}{2}\right)$ com $a, b \in \mathbb{Z}$ ímpares (e portanto $a^2 \equiv b^2 \equiv 1 \pmod 4$), vem que

$$n = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = \frac{a^2 + b^2}{4} \Leftrightarrow 4n = a^2 + b^2.$$

Reduzindo esta igualdade módulo 4 obtém-se

$$0 \equiv 4n \equiv a^2 + b^2 \equiv 2 \pmod 4,$$

o que é absurdo. Conclui-se assim que não existem pontos em $\mathcal{Q}_n$ com coordenadas na forma irredutível cujo denominador é 2. □

Aliás, substituindo o denominador na prova anterior por $2^k l$, em que $k, l \in \mathbb{N}$ e l é ímpar, verifica-se que $\mathcal{Q}_n$ não tem pontos com denominador par.

Vejamos agora que se a recta que passa pelo ponto P de $\mathcal{Q}_n$ e o ponto de coordenadas inteiras que lhe é mais próximo não for tangente à circunferência e tiver declive racional, então intersecta $\mathcal{Q}_n$.

Proposição 3.4. *Seja* $P \in \mathcal{Q}_n$ *e seja* r *uma recta de declive racional que passa em* P. *Se* r *intersecta* $\mathcal{C}_n$ *num outro ponto* P', *então* P' *também tem coordenadas racionais.*

Demonstração. Seja $v \in \mathbb{Z}^2$ o vector director da recta r. A interseção de $\mathcal{C}_n$ com a recta r é o ponto P' que satisfaz

$$\begin{cases} P' = \lambda v + P \\ ||P'||^2 = ||P||^2, \end{cases} \tag{3.1}$$

para algum $\lambda \in \mathbb{R}$.

Substituindo P' da segunda equação por $\lambda v + P$ obtém-se

$$||P||^2 = (\lambda v + P) \cdot (\lambda v + P) = \lambda^2 ||v||^2 + ||P||^2 + 2\lambda(v \cdot P),$$

onde $\cdot$ denota aqui o produto interno.
Ou seja, para que a recta intersecte $\mathcal{C}_n$ num outro ponto P', tem que existir λ tal que:

$$\lambda\left(\lambda||v||^2 + 2(v \cdot P)\right) = 0.$$

Se $\lambda = 0$, então o resultado da interseção é obviamente P. A outra raíz

$$\lambda = -2\frac{v \cdot P}{||v||^2} \tag{3.2}$$

é ainda nula se $v \cdot P = 0$. Portanto para que haja uma segunda interseção, a recta r não pode ser tangente à circunferência.

Neste caso r intersecta $\mathcal{C}_n$ no ponto

$$P' = -2\frac{v \cdot P}{||v||^2}v + P. \tag{3.3}$$

Como $v \in \mathbb{Z}^2$ resulta que P' tem coordenadas racionais. □

No que se segue, utilizaremos $[q]$ para denotar o número inteiro mais próximo de $q \in \mathbb{Q}$, sendo irrelevante o arredondamento que se toma para os números da forma $k+\frac{1}{2}$, com $k \in \mathbb{Z}$, pois não existem pontos de $\mathcal{Q}_n$ com denominador 2.

Os números considerados neste trabalho são da forma $N = pq$ tais que p, q são primos distintos decomponíveis em soma de dois quadrados, representando assim os números compostos com o menor número de produtos de factores primos.

Mostremos que, para estes números, a recta definida por um ponto P de coordenadas racionais e pelo ponto de coordenadas inteiras que lhe é mais próximo não é tangente a $\mathcal{Q}_n$.

Lema 3.5. *Seja $S \in \mathcal{Q}_n$, com $n = pq$ onde p, q são primos distintos. Se $S \notin \mathbb{Z}^2$, então a recta que passa por S e pelo ponto de coordenadas inteiras que lhe é mais próximo não é tangente a $\mathcal{Q}_n$.*

Demonstração. Pela proposição anterior, se a recta que passa por S e pelo ponto de coordenadas inteiras que lhe é mais próximo intersecta $\mathcal{C}_n$ num segundo ponto, então esse ponto tem coordenadas racionais, ou seja, se a recta não for tangente a $\mathcal{C}_n$, então não é tangente a $\mathcal{Q}_n$.

Suponha-se que $S = (x, y) \in \mathcal{Q}_n \backslash \mathbb{Z}^2$ é tal que a recta definida por (x, y) e $([x], [y])$ é tangente a $\mathcal{C}_n$. Segue assim que:

$$(x, y) \cdot (([x], [y]) - (x, y)) = 0 \Leftrightarrow [x]\, x + [y]\, y - x^2 - y^2 = 0 \Leftrightarrow [x]\, x + [y]\, y = n.$$

Por isso, a interseção dessa recta com a circunferência $\mathcal{C}_n$ satisfaz o seguinte sistema de equações:

$$\begin{cases} [x]\,x + [y]\,y = n \\ x^2 + y^2 = n. \end{cases}$$

Multiplicando todos os elementos na segunda equação por $[y]^2$ tem-se

$$([y]\,x)^2 + ([y]\,y)^2 = [y]^2 n \Leftrightarrow ([y]\,x)^2 + (n - [x]\,x)^2 = [y]^2 n$$

e por fim segue que

$$\left([x]^2 + [y]^2\right) x^2 - 2[x]\,nx + \left(n^2 - [y]^2 n\right) = 0.$$

Uma vez que esta é uma equação de segundo grau, para que x seja racional, o binómio discriminante deve ser um número quadrado. Como

$$\Delta = 4[x]^2 n^2 + 4\left([x]^2 + [y]^2\right)\left([y]^2 n - n^2\right) = 4[y]^2 n\left([x]^2 + [y]^2 - n\right),$$

para que Δ seja um quadrado, o número $n\left([x]^2 + [y]^2 - n\right)$ também o tem de ser. Como n é livre de quadrados, então deverá ter-se que

$$[x]^2 + [y]^2 - n = k^2 n \geq n,$$

para algum $k \in \mathbb{N}$.
Como $[x] = x + \epsilon$ e $[y] = y + \sigma$, com $|\epsilon|, |\sigma| < \frac{1}{2}$, resulta que

$$[x]^2 + [y]^2 - n = 2(x\epsilon + y\sigma) + \epsilon^2 + \sigma^2.$$

Relembre-se que não existem pontos de $\mathcal{Q}_n$ com denominador 2, e daí $|\epsilon|, |\sigma| \neq \frac{1}{2}$.
Como n é livre de quadrados, então $x^2, y^2 < n$, logo $|x|, |y| < \sqrt{n}$. E assim:

$$\left|[x]^2 + [y]^2 - n\right| \leq 2(|x||\epsilon| + |y||\sigma|) + \epsilon^2 + \sigma^2 < 2\sqrt{n} + \frac{1}{2}.$$

Ou seja,

$$n \leq \left|[x]^2 + [y]^2 - n\right| < 2\sqrt{n} + \frac{1}{2},$$

o que é falso para $n > 5$. Como não existe nenhum número inferior a 6 que seja um produto de dois primos distintos, então não existem rectas tangentes nas condições impostas. □

Portanto, se tomarmos um ponto de coordenadas racionais mas não inteiras em $\mathcal{C}_n$, para $n = pq$ como acima, então a recta que passa por esse ponto e o ponto de coordenadas inteiras mais próximo não é tangente e intersecta $\mathcal{C}_n$ num ponto de coordenadas racionais. Vejamos agora que esse segundo ponto tem um denominador menor que o primeiro.

Proposição 3.6. *Sejam $n = pq$ como acima e $S = (s_1, s_2) \in \mathcal{Q}_n$ tal que $s_1, s_2 \in \mathbb{Q}\backslash\mathbb{Z}$ e seja ainda $R = ([s_1], [s_2])$. Então a recta definida por S e R intersecta $\mathcal{Q}_n$ num outro ponto S' cujo denominador é inferior a metade do denominador de S.*

Demonstração. Como $S, R \in \mathbb{Q}^2$, então a recta que intersecta S e R tem declive racional, e assim pela proposição 3.4, S' tem coordenadas racionais, ou seja, pertence a $\mathcal{Q}_n$.
A interseção de $\mathcal{Q}_n$ com a recta definida por S e R satisfaz o seguinte sistema de equações:

$$\begin{cases} S' = R + \lambda(S - R) = \lambda S + (1 - \lambda)R \\ ||S'||^2 = n. \end{cases} \tag{3.4}$$

Se $\lambda = 0$, então $R \in \mathcal{Q}_n$, isto é, o ponto de coordenadas inteiras mais próximo de S corresponde à segunda intersecção da recta com $\mathcal{C}_n$. Como o denominador de R é 1 e o denominador de S é, no mínimo, 3 pela proposição 3.3, a proposição fica provada para esta situação.
Caso $\lambda \neq 0$, substituindo S' por $S' = R + \lambda(S - R) = \lambda S + (1 - \lambda)R$ na segunda equação, tem-se que

$$n = ||\lambda S + (1 - \lambda)R||^2,$$

de onde resulta, com $\cdot$ denotando o produto interno,

$$n = \lambda^2||S||^2 + (1 - \lambda)^2||R||^2 + 2\lambda(1 - \lambda)S \cdot R$$

$$\Leftrightarrow (1 - \lambda^2)n = (1 - \lambda)^2||R||^2 + 2\lambda(1 - \lambda)R \cdot S.$$

Com $\lambda \neq 1$, segue que

$$(1 + \lambda)n = (1 - \lambda)||R||^2 + 2\lambda R \cdot S$$

$$\Leftrightarrow \lambda(n + ||R||^2 - 2R \cdot S) = ||R||^2 - n$$

$$\Leftrightarrow \lambda||S - R||^2 = ||R||^2 - n.$$

E por fim

$$\lambda = \frac{||R||^2 - n}{||S - R||^2}.$$

Substituindo λ na equação da recta vem finalmente que

$$S' = R + \frac{||R||^2 - n}{||S - R||^2}(S - R).$$

Sendo $b \in \mathbb{N}$ o denominador de S, e $S^* \in \mathbb{Z}^2$ tal que $S = \frac{1}{b}S^*$, então tem-se que

$$S' = R + \frac{b(||R||^2 - n)}{b||S - R||^2}(S - R) = R + \frac{||R||^2 - n}{b||S - R||^2}(S^* - bR).$$

Observemos que $b||S-R||^2 = b(||S||^2+||R||^2)-2b(S\cdot R) = b(||S||^2+||R||^2)-2(S^*\cdot R) \in \mathbb{N}$. Dado que $||R||^2 - N \in \mathbb{Z}$ e que $(S^* - bR) \in \mathbb{Z}^2$, então $b||S-R||^2$ é um múltiplo do denominador de S'. Para finalizar falta comparar os denominadores de S e S'.

Acontece que $||S-R||^2$ é máximo quando as coordenadas de S são da forma $k+\frac{1}{2}$, porém pela proposição 3.3, esse máximo nunca é atingido. Logo

$$||S-R||^2 < \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{4}+\frac{1}{4} = \frac{1}{2}. \tag{3.5}$$

Sendo $b' \in \mathbb{N}$ o denominador de S', conclui-se que

$$b' \leq b||S-R||^2 < \frac{1}{2}b < b.$$

Portanto, o denominador de S' é menor que metade do denominador de S. □

Pela demonstração da proposição anterior é possível explicitar as coordenadas do ponto S', e assim tem-se uma expressão para a função $f : \mathcal{Q}_n \to \mathcal{Q}_n$ que retorna a interseção da recta definida por $S = (x, y)$ e por $R = ([x], [y])$ com $\mathcal{Q}_n$:

$$f(S) = \begin{cases} S' = R + \frac{||R||^2-n}{||S-R||^2}(S-R) & \text{se } S \notin \mathbb{Z}^2 \\ S & \text{se } S \in \mathbb{Z}^2. \end{cases}$$

Dado que o denominador de S' é menor que S, então se aplicarmos várias vezes a função f, a certa altura obtém-se um ponto de coordendas inteiras.

Portanto, o algoritmo de Aubry é dado pela função:

$$\mathcal{A}(P) = f^m(P), \text{ onde } m = min\{k \in \mathbb{N} : f^k(P) \in \mathbb{Z}^2\}$$

com $P \in \mathcal{Q}_n$.

O algoritmo de Aubry faz assim corresponder, a cada ponto de $\mathcal{Q}_n$, um ponto de coordenadas inteiras dessa mesma circunferência. Como cada ponto de coordenadas inteiras corresponde a uma decomposição de n em soma de dois quadrados, então é possível obter-se uma decomposição de n em soma de dois quadrados a partir de qualquer ponto de $\mathcal{Q}_n$.

A figura 3.2 ilustra o procedimento do Algoritmo de Aubry aplicado num ponto de $\mathcal{Q}_{65}$: o ponto inicial é $S_0 = (-7231/929, -1952/929)$, $S_1 = f(S_0) = (179/53, -388/53)$, $S_2 = f(S_1) = (-101/13, 28/13)$ e o ponto final $S_3 = \mathcal{A}(S_0) = (1, 8)$. Os pontos azuis próximos dos pontos assinalados correspondem aos pontos de coordenadas inteiras mais próximos que a função f considera.

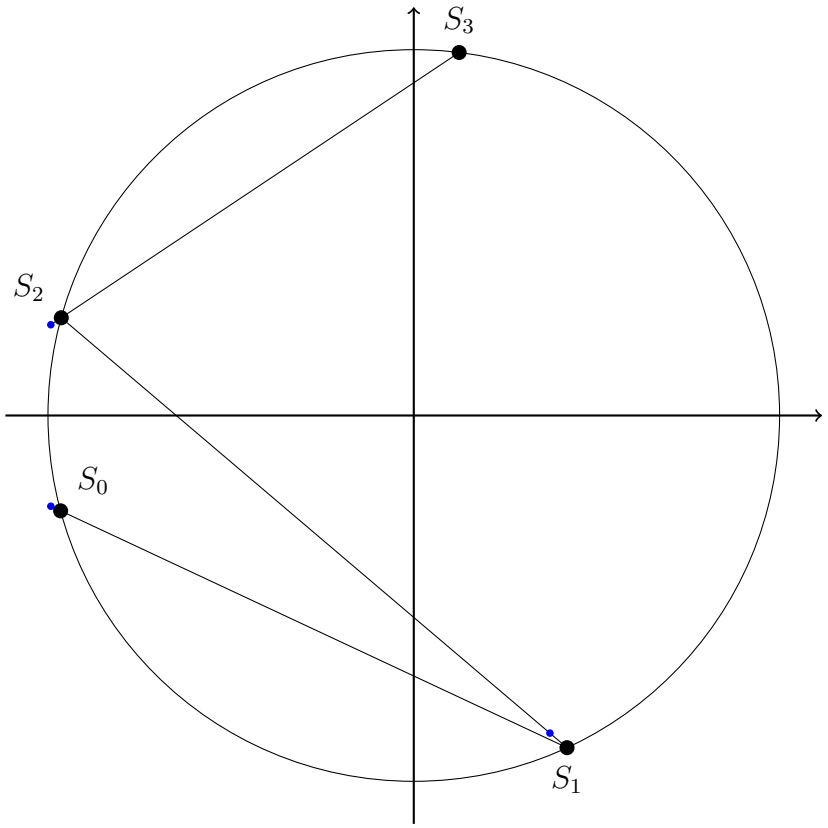

Figura 3.2: Exemplo de uma aplicação do Algoritmo de Aubry em $\mathcal{Q}_{65}$

3.2 Classes de Aubry

Existem pontos distintos de coordenadas inteiras de $\mathcal{Q}_n$ que correspondem à mesma decomposição de n em soma de dois quadrados. Em particular, trocando as coordenadas ou os sinais de um ponto de coordenadas inteiras (a, b), os pontos que se obtêm correspondem à mesma soma de dois quadrados. Se $a \neq b$, o que necessariamente acontece no caso de se ter $n = pq$, com p e q primos ímpares distintos, têm-se oito pontos que, em certo sentido, correspondem à mesma decomposição como soma de dois quadrados.

Definição 3.7. *Seja* $(a, b) \in \mathcal{Q}_n$. *Designaremos por* pontos associados *a* (a, b) *os pontos pertencentes ao conjunto*

$$\mathcal{S}((a, b)) = \{(x, y) \in \mathcal{Q}_n : (|x|, |y|) = (|a|, |b|) \vee (|x|, |y|) = (|b|, |a|)\}.$$

Se $(a,b) \in \mathcal{Q}_n \cap \mathbb{Z}^2$, os seus pontos associados correspondem à mesma decomposição em soma de dois quadrados.
É claro que o conjunto $\mathcal{Q}_n \cap \mathbb{Z}^2$ é finito, sendo uma reunião disjunta de um número finito de conjuntos de associados, ou seja,

$$\mathcal{Q}_n \cap \mathbb{Z}^2 = \coprod_{i=1}^{k} \mathcal{S}(P_i), \tag{3.6}$$

para alguns $P_i \in \mathcal{Q}_n$.

Se $S_1, S_2 \in \mathcal{Q}_n$ forem distintos e tais que $\mathcal{A}(S_1) \neq \mathcal{A}(S_2)$ e $\mathcal{S}(\mathcal{A}(S_1)) = \mathcal{S}(\mathcal{A}(S_2))$, então S_1 e S_2 conduzem à mesma decomposição em soma de dois quadrados inteiros. Como estamos interessado em procurar decomposições essencialmente distintas, introduzimos a seguinte relação de equivalência:

$$S_1 \sim S_2 \iff \mathcal{S}(\mathcal{A}(S_1)) = \mathcal{S}(\mathcal{A}(S_2)).$$

Definição 3.8. *As classes de equivalência geradas pela relação $\sim$ designam-se por* classes de Aubry. *As classes em $\mathcal{Q}_n$ serão denominadas classes de Aubry de n.*

É fácil ver que os primos da forma $4k+1$ têm somente uma classe de Aubry e o produto de dois primos dessa forma têm exactamente duas classes de Aubry. Pelo teorema 2.28, se um número tiver (pelo menos) duas classes de Aubry distintas, então esse número é composto.

Observemos agora que para quaisquer $P, Q \in \mathcal{Q}_n$ tais que $Q \sim P$, se tem $\mathcal{A}(Q) \sim \mathcal{A}(P)$. Para ver isto basta mostrar que $Q \sim P \Rightarrow f(Q) \sim f(P)$.

De facto, sejam $P = (p_1, p_2)$ e $R = ([p_1], [p_2]) = (r_1, r_2)$. As coordenadas de $f(P) = P' = (p_1', p_2')$ são as seguintes:

$$p_i' = r_i + \frac{||(r_1,r_2)||^2 - n}{||(p_1 - r_1, p_2 - r_2)||^2}(p_i - r_i) = [p_i] + \frac{||R||^2 - n}{||P-R||^2}(p_i - [p_i]), \tag{3.7}$$

com $i \in \{1,2\}$.

Portanto podemos reescrever a função f como $f(P) = f(p_1,p_2) = (p_1', p_2') = (\sigma_1(p_1), \sigma_2(p_2))$, onde $\sigma_i : \mathbb{Q} \to \mathbb{Q}$ é tal que $\sigma_i(p_i) = p_i'$. Da equação (3.7), resulta que $\sigma_1 = \sigma_2$. Denotaremos esta função por σ.

Primeiro vejamos qual o valor de $f(Q)$ se Q corresponder à mudança de um ou dos dois sinais de P.
Se $q_i = -p_i$, segue que $[-p_i] = -[p_i] = -r_i$, pois p_i não é da forma $k + \frac{1}{2}$. Como $(-r_i)^2 = (r_i)^2$ e $(-p_i - (-r_i))^2 = (p_i - r_i)^2$, então não existem alterações nas normas de R e de $P - R$.

Agora tem-se

$$\begin{aligned}\sigma(-p_i) &= -r_i + \frac{||R||^2 - n}{||P-R||^2}(-p_i + r_i) \\ &= -\left[r_i + \frac{||R||^2 - n}{||P-R||^2}(p_i - r_i)\right] = -\sigma(p_i).\end{aligned}$$

Portanto $\sigma^2(-p_i) = \sigma(\sigma(-p_i)) = \sigma(-\sigma(p_i)) = -\sigma^2(p_i)$. Logo para todo $k \in \mathbb{N}$, tem-se que $\sigma^k(-p_i) = -\sigma^k(p_i)$.

Assim sendo, ao mudar o sinal da i-ésima coordenada de $P \in \mathcal{Q}_n$, o sinal da i-ésima coordenada de $\mathcal{A}(P)$ também se altera, e assim pertence a $\mathcal{S}(\mathcal{A}(P))$.

No caso de se trocarem as coordenadas de P, isto é, $Q = (p_2, p_1) \in \mathcal{Q}_n$, segue que:

$$f(Q) = (\sigma(p_2), \sigma(p_1)),$$

por isso tem-se:

$$\mathcal{A}(Q) = f^n(Q) = (\sigma^n(p_2), \sigma^n(p_1))$$

e assim as coordenadas em $\mathcal{A}(P)$ também vão trocar de posição.

É agora claro que a composição de mudança de sinal com a mudança da posição das coordenadas de P afeta de igual modo as coordenadas $\mathcal{A}(P)$.

Portanto conclui-se que aplicando o algorimo de Aubry a qualquer associado de P, obtém-se um associado de $\mathcal{A}(P)$. Ou seja, os elementos de $\mathcal{S}(P)$ pertencem à mesma classe de Aubry. Portanto, conhecendo a classe de Aubry de todos os pontos racionais do maior arco em $\mathcal{C}_n$ que não contém pontos associados entre si, sabem-se as classes de todos os pontos de $\mathcal{Q}_n$. Por exemplo, conhecendo as classes de Aubry dos pontos de $\mathcal{Q}_n$ no primeiro octante, tem-se conhecimento das classes de todos os pontos racionais da circunferência.

Será possível medir o comprimento de cada classe de Aubry? Não conseguimos responder a esta pergunta, mas vamos mostrar que as classes são mensuráveis.

Para o provar, considere-se $P_0 \in \mathcal{Q}_n$ tal que $\mathcal{A}(P_0) = f^m(P_0) = P_m \in \mathcal{Q}_n \cap \mathbb{Z}^2$ com $m > 0$ e sejam $P_i = (x_i, y_i) = f^i(P_0)$, com $i \in \{1, ..., m-1\}$. Seja $Q_i = ([x_i], [y_i])$ o ponto de coordenadas inteiras mais próximo de P_i. Em particular, $P_m = Q_m$.
Observe-se que o conjunto $B\left(Q_i; \frac{1}{2}\right) = \left\{P \in \mathcal{Q}_n : ||P - Q_i||_\infty < \frac{1}{2}\right\}$, onde $||\cdot||_\infty$ é a norma do supremo em $\mathbb{R}^2$, corresponde à região de pontos racionais que têm Q_i como o ponto de coordenadas inteiras mais próximo. Note-se que não se incluem os pontos com pelo menos uma coordenada da forma $k + \frac{1}{2}$ para algum $k \in \mathbb{Z}$, pois pela proposição 3.3, esse tipo de

pontos não pertence a $\mathcal{Q}_n$. O conjunto $B\left(Q_i;\frac{1}{2}\right)$ é um aberto e se $P \in B\left(P_m;\frac{1}{2}\right)$, então $f(P) = P_m$.

Relembre-se que $f : \mathcal{C}_n \longrightarrow \mathcal{C}_n$ é dado por:

$$f(S) = \begin{cases} S' = R + \frac{||R||^2-n}{||S-R||^2}(S-R) = g(S) + \frac{||g(S)||^2-N}{||S-g(S)||^2}(S-g(S)) & \text{se } S \notin \mathbb{Z}^2 \\ S & \text{se } S \in \mathbb{Z}^2, \end{cases}$$

em que $g : \mathcal{C}_n \longrightarrow \mathcal{Q}_n \cap \mathbb{Z}^2$, é dado por $g((x,y)) = ([x],[y])$, para qualquer $(x,y) \in \mathcal{C}_n$, onde aqui se toma $\left[k+\frac{1}{2}\right] = k+1$, para todo $k \in \mathbb{Z}$ (esta escolha não afecta o valor de f em nenhum ponto de $\mathcal{Q}_n$, pela proposição 3.3). Isto é, g aplica a função $[-] : \mathbb{R} \longrightarrow \mathbb{Z}$ coordenada a coordenada, que é uma função em escada.
Assim o conjunto dos números da forma $k+\frac{1}{2}$ são exactamente os pontos de descontinuidade de $[-]$, pontos esses que não existem em $\mathcal{Q}_n$, e por conseguinte g é contínua em $\mathcal{Q}_n$.

Com esta observação, verifica-se que o primeiro ramo de f é dado por uma composição de várias funções contínuas e, por isso, é também uma função contínua.
Dado $S \in \mathcal{Q}_n \cap \mathbb{Z}^2$, é imediato que $\forall T \in B\left(S,\frac{1}{2}\right)$, $f(T) = S$, ou seja, f é constante nos pontos de uma vizinhança de S.
Conclui-se assim que f é uma função contínua.

Seja $L_{m-1} = B\left(Q_{m-1};\frac{1}{2}\right) \cap f^{-1}\left(B\left(Q_m;\frac{1}{2}\right)\right)$ o conjunto de pontos da vizinhança de P_{m-1} que têm Q_{m-1} como o ponto de coordenadas inteiras mais próximo e tais que $f^2(P) = Q_m$, com $P \in L_{m-1}$. Como f é contínua, então $f^{-1}\left(B\left(Q_m;\frac{1}{2}\right)\right)$ é também um aberto. E dado que a interseção de dois abertos é também um aberto, então L_{m-1} é um aberto.
Sejam agora $L_j = B\left(Q_j;\frac{1}{2}\right) \cap f^{-1}(L_{j+1})$, com $j \in \{0,...,m-2\}$, que são todos abertos, por indução.

Em particular, L_0 é um aberto e portanto existe uma vizinhança de P_0 tal que todos os pontos dessa vizinhança que estão em $\mathcal{C}_n$ pertencem todos à mesma classe de P_0. Conclui-se então que para qualquer ponto de $\mathcal{Q}_n$, existe uma vizinhança desse ponto que pertence à mesma classe de Aubry. Logo as componentes conexas das classes de Aubry são abertas.

Vê-se assim que, para cada classe de Aubry $\mathcal{X}$, existe um aberto $\mathcal{U}_\mathcal{X}$ de $\mathcal{C}_n$ tal que $\mathcal{X} = \mathcal{U}_\mathcal{X} \cap \mathcal{Q}n$ e que, sendo aberto e estando contido em $\mathcal{C}_n$, é mensurável [1, Chap. 2, Sections 10–12], tendo obviamente medida finita. Faz assim sentido falar da medida de $\mathcal{X}$, que será a de $\mathcal{U}_\mathcal{X}$, e da proporção de pontos em $\mathcal{X}$ que será $\frac{\mathfrak{m}(\mathcal{U}_\mathcal{X})}{2\pi\sqrt{n}}$.

Isto coloca, naturalmente, as questões seguintes. Havendo mais que uma classe de Aubry, estas terão medidas iguais? Se não tiverem, qual é a proporção que cada uma delas tem com o perímetro de $\mathcal{C}_n$? No capítulo 4 estas questões são investigadas de um ponto de vista computacional.

3.3 Generalização de Davenport e Cassels

O algoritmo de Aubry fornece pontos de coordenadas inteiras da circunferência de raio $\sqrt{n}$ centrada na origem, com $n \in \mathbb{N}$, a partir de pontos de coordenadas racionais dessa mesma circunferência. Acontece que se pode usar o mesmo método para superfícies esféricas, em $\mathbb{R}^3$, centradas na origem e de raio $\sqrt{n}$. Assim, a partir de uma decomposição de n como soma de três quadrados racionais é sempre possível obter uma decomposição como soma de três quadrados inteiros. Já em $\mathbb{R}^4$ isso não acontece (ver p. 31).

Os matemáticos John Cassels e Harold Davenport descobriram que se podia aplicar um método idêntico ao algoritmo de Aubry noutros anéis, desde que estes satisfizessem umas certas condições.

Em primeiro lugar, o anel escolhido deve admitir uma norma multiplicativa.

Definição 3.9. *Seja R um anel comutativo com unidade $1 \neq 0$.*
Uma norma discreta multiplicativa em R é uma função $|-| : R \to \mathbb{N}$ que satisfaz as seguintes duas condições:

- *para todo $x \in R$, $|x| = 0$ sse $x = 0$;*
- *para quaisquer $x, y \in R$, $|xy| = |x||y|$.*

Como $|1| \cdot |1| = |1 \cdot 1| = |1| \neq 0$, tem-se que $|1| = 1$, e assim $|-|$ é um homomorfismo de monóides multiplicativos.
Seja $|-|$ uma norma discreta multiplicativa em R. Se x e y são elementos não-nulos de R, então $|xy| = |x| \cdot |y| \neq 0$, portanto $xy \neq 0$ e por isso o anel R é um domínio de integridade. Seja K o corpo de frações de R. É possível extender de uma única maneira a função $|-|$ a $|-| : K \to \mathbb{Q}^{\geq 0}$, satisfazendo as mesmas condições, pondo-se $|x| = |a|/|b|$, para $x = a/b$ com $a, b \in R$ e $b \neq 0$.

O que Cassels e Davenport fizeram foi extender o método de Aubry para outras formas mais gerais que $x^2 + y^2$ e a outros anéis além de $\mathbb{Z}$. Comecemos por relembrar a noção de "forma".

Definição 3.10. *Uma* forma *sobre um anel R é um polinómio homogéneo de $R[x_1, ..., x_d]$ $(d > 0)$, em que x_i são variáveis formais. Se o grau de todos os monómios for 2 a forma diz-se uma* forma quadrática.

Para simplificar a notação, pomos $X = [x_1, ..., x_d]$ e $Y = [y_1, ..., y_d]$. Seja $q \in R[x_1, ..., x_d]$ uma forma quadrática. O polinómio

$$\langle X, Y \rangle_q := q(X + Y) - q(X) - q(Y) \in R[x_1, ..., x_d, y_1, ..., y_d]$$

é uma forma bilinear, ou seja, linear em cada uma das duas variáveis X e Y. Se t é uma variável formal diferente de todas as variáveis formais x_i e y_i, tem-se que

$$q(X+tY) = q(X) + \langle X, tY\rangle_q + q(tY),$$

e fazendo $q(X) = \sum_{i,j=1}^{d} c_{i,j}x_jx_i$, vem que $\langle X, Y\rangle_q = \sum_{i,j=1}^{d} c_{i,j}(x_iy_j + x_jy_i)$ e assim

$$\langle X, tY\rangle_q = \sum_{i,j=1}^{d} c_{i,j}[(x_i+ty_i)(x_j+ty_j) - x_ix_j - t^2y_iy_j] = \sum_{i,j=1}^{d} c_{i,j}t(x_iy_j + x_jy_i).$$

Portanto $\langle X, tY\rangle_q = \langle X, Y\rangle_q t$.

Além disso, como q é uma forma quadrática, então $q(tY) = t^2q(Y)$ e segue que

$$q(X+tY) = q(X) + \langle X, Y\rangle_q t + q(Y)t^2.$$

O facto do coeficiente de t^2 ser $q(Y)$, será útil na prova do teorema abaixo.

Seja R um domínio de integridade com o corpo de frações K.

Definição 3.11. *Uma* forma ADC *é uma forma g sobre R, em d variáveis, que satisfaz a seguinte condição, para todo $X \in K^d$:*

$$g(X) \in R \Rightarrow \exists Y \in R^d : g(Y) = g(X).$$

Ou seja, uma forma diz-se ADC *se sempre que a equação $g(X) = c$, com $c \in R$, tiver solução em K^d, então também tem solução em R^d.*

Seja $|-|$ uma norma discreta multiplicativa em R extendida (de forma única) para uma norma multiplicativa em K (escrevendo-se ainda $|-|$).

Definição 3.12. *Uma forma g sobre R, de qualquer grau, diz-se* Euclideana com respeito a $|-|$ *se, para todo $X \in K^d \backslash R^d$, existe $Y \in R^d$ tal que $0 < |g(X-Y)| < 1$.*

Teorema 3.13. *Seja R um domínio de integridade, com corpo de frações K, e seja $|-|$ uma norma discreta multiplicativa em R. Seja $f = f_2 + f_1 + f_0 \in R[x_1, ..., x_d]$, onde f_i é homogéneo de grau i, e f_2 é Euclidiano com respeito a $|-|$. Se f tem um zero em K^d, então tem um zero em R^d.*

Demonstração. Seja $X \in K^d$ um zero de f. Se $X \in R^d$ não há nada a provar. Suponhamos pois que $X \notin R^d$.

Tem-se que $X = A/d$ para algum $A \in R^d$ e $d \in R\backslash\{0\}$. Como f_2 é Euclidiano com respeito a $|-|$, existe $Y \in R^d$ tal que $0 < |f_2(X-Y)| < 1$. Faça-se $X-Y = V/d$ com $V = A-dY \in R^d$. Seja agora $F(t) := f(Y+tV) = at^2 + bt + c$, para $t \in K$.

O coeficiente c determina-se facilmente: $c = F(0) = f(Y)$.
O coeficiente a advém apenas de f_2. Tem-se que as parcelas de $f_2(Y + tV)$ são da forma $(y_i + tv_i)(y_j + tv_j) = y_i y_j + (v_i y_j + v_j y_i)t + v_i v_j t^2$ com $i, j \in \{1, ..., d\}$. Portanto, o coeficiente de t^2 em $f_2(Y + tV)$ é $f_2(V)$, ou seja, $a = f_2(V)$.
Segue que $a = f_2(V) = f_2(d(X - Y)) = d^2 f_2(X - Y) \neq 0$, pois $|f_2(X - Y)| > 0$ e $d \neq 0$.
Por fim, $b = f(Y + V) - a - c$. Vê-se assim que todos os coeficientes pertencem a R.

Sabe-se que $\tau := 1/d$ é um zero de F porque $X = Y + V/d$. Denote-se por τ' o outro zero de F. Como $\tau\tau' = c/a$, tem-se que $\tau' = c/(\tau a) = c/(a/d)$, e

$$dF(\tau) = a/d + b + cd \Leftrightarrow a/d = -b - cd$$

que pertence a R. Segue que $a/d = f_2(X - Y)d$, em que $|a/d| = |f_2(X - Y)||d| < |d|$.

O ponto $X' := Y + \tau' V$ é um zero de f, e $X' = A'/d'$, em que $d' = a/d \in R\backslash\{0\}$, $A' = d'Y + cV \in R^d$ e $|d'| < |d|$.

Se o zero X' de f ainda não pertence a R, repete-se o procedimento e obtém-se um outro zero $X'' = A''/d''$ de f, com $A'' \in R^d$, $d'' \in R\backslash\{0\}$, e $|d''| < |d'|$. Iterando este processo, obtém-se uma sequência X, X', X'', ... de zeros de f que tem de terminar com um zero $X^* \in R^d$ de f, pois $|d| > |d'| > |d''| > ...$. □

Em particular, tem-se o seguinte corolário.

Corolário 3.14. *Seja R um domínio de integridade com uma norma discreta multiplicativa $|-|$. Se a forma quadrática q sobre R é Euclideana com respeito a $|-|$, então é uma forma ADC.*

Demonstração. Dado um $r \in R$, aplica-se o teorema acima para $q - r$. □

3.4 Exemplos

A forma $x^2 + y^2$ pertence a $\mathbb{Z}[x, y]$ e é Euclideana com respeito a $|-|$, pois para qualquer ponto $(x, y) \in \mathbb{Q}^2$, o ponto de coordenadas inteiras que lhe é mais próximo está a uma distância inferior a $\frac{1}{2}$, como se viu em (3.5). Portanto, $x^2 + y^2$ é uma forma ADC. Vê-se assim, novamente, que qualquer circunferência centrada na origem representada pela curva de nível $x^2 + y^2 = n$, com $n \in \mathbb{N}$, tem pontos de coordenadas inteiras se tiver, pelo menos, um ponto de coordenadas racionais. Isto é, se $\mathcal{Q}_n \neq \emptyset$, então $\mathcal{Q}_n \cap \mathbb{Z}^2 \neq \emptyset$.

Em relação à forma $g(x, y, z) = x^2 + y^2 + z^2$, que pertence a $\mathbb{Z}[x, y, z]$, sejam $P \in \mathbb{Q}^3$ e $Q \in \mathbb{Z}^3$ o ponto de coordenadas inteiras mais próximo de P. Então tem-se que:

$$|g(P - Q)|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{3}{4},$$

logo a forma $g(x,y,z)$ é Euclideana com respeito a $|-|$, e por isso também é ADC. Ou seja, se a circunferência em $\mathbb{R}^3$, centrada na origem e de raio $\sqrt{n}$, tiver um ponto de coordenadas racionais, então tem um ponto de coordenadas inteiras. De facto, o método de Aubry neste caso pode ser também usado.

Já a forma $h(x,y,z,w) = x^2+y^2+z^2+w^2 \in \mathbb{Z}[x,y,z,w]$ não é Euclideana para $|-|$, pois para qualquer ponto P cujas coordenadas são todas da forma $k+\frac{1}{2}$, para algum $k \in \mathbb{Z}$, e para qualquer ponto de coordenadas inteiras Q, tem-se

$$|h(P-Q)| \geq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1.$$

Pode-se mostrar que h é Euclideana quando considerada sobre o anel dos inteiros de Hurwitz:

$$\mathcal{H} = \left\{(x,y,z,w) \in \mathbb{R}^4 : x,y,z,w \in \mathbb{Z} \vee x,y,z,w \in \mathbb{Z}+\frac{1}{2}\right\}.$$

Vejamos agora como determinar alguns valores de $d \in \mathbb{Z}$, d livre de quadrados, para os quais a forma x^2-dy^2 é ADC.
Para tal, seja $R = \mathbb{Z}[\sqrt{d}]$, sendo $K = \mathbb{Q}[\sqrt{d}]$ o seu corpo de frações. Considere-se a aplicação $\mathrm{N} : \mathbb{Q}[\sqrt{d}] \longrightarrow \mathbb{N}_0$ dada por $\mathrm{N}(x+y\sqrt{d}) = |x^2-dy^2| = |(x+y\sqrt{d})(x-y\sqrt{d})|$, com $x,y \in \mathbb{Q}$.

Verifiquemos que as condições da definição de norma discreta multiplicativa são cumpridas pela aplicação N. Tem-se

$$\mathrm{N}(x+y\sqrt{d}) = |x^2-dy^2| = 0 \Leftrightarrow x^2 = dy^2$$

como d é livre de quadrados, $\mathrm{N}(z) = 0$ sse $z = 0$.

Para $\alpha = x+y\sqrt{d}$, ponha-se $\overline{\alpha} = x-y\sqrt{d}$. Observe-se que $\mathrm{N}(\alpha) = |\alpha\overline{\alpha}|$ e $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$.
Agora, sendo $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ tem-se

$$\mathrm{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

Conclui-se assim que o operador N é uma norma discreta multiplicativa.

Seja $S_n = \left\{\alpha \in \mathbb{Q}[\sqrt{d}] : \mathrm{N}(\alpha) = n\right\}$ o conjunto de todos os pontos do anel referido com norma igual a n, ou seja, a "circunferência" em $\mathbb{Q}[\sqrt{d}]$ centrada na origem e com raio $\sqrt{n}$ (de facto, no plano Euclideano esta "circunferência" é ou uma elipse, se $d > 0$, ou uma hipérbole se $d < 0$ e $d \neq 1$).

Dado $\alpha \in \mathbb{Q}[\sqrt{d}]$, pode-se sempre escrever $\alpha = (a+\epsilon)+(b+\phi)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, onde $a,b \in \mathbb{Z}$ e $\epsilon, \phi \in \mathbb{Q}$ são tais que $|\epsilon|, |\phi| \leq \frac{1}{2}$.

O elemento de $\mathbb{Z}[\sqrt{d}]$ mais próximo de α é pois $\delta = a + b\sqrt{d}$.

Portanto, para que a forma $x^2 - dy^2$ seja Euclideana com respeito a $\mathrm{N}(\cdot)$, basta que $\mathrm{N}(\alpha - \delta) < 1$. Mas

$$\mathrm{N}(\alpha - \delta) = |\epsilon^2 - d\phi^2| \leq \frac{1}{4} + \frac{|d|}{4} = \frac{|d|+1}{4} < 1 \Leftrightarrow |d| < 3.$$

Por conseguinte, para $d = -2, -1, 1, 2$, vem que $x^2 - dy^2$ é Euclidiana com respeito à norma N.

Vejamos agora que o método de Aubry também pode ser usado nestes anéis, procedendo de um modo análogo ao que foi feito na secção 3.1. Tal como em $\mathcal{Q}_n$, verifiquemos que as coordenadas dos pontos da "circunferência" S_n têm o mesmo denominador.

Se $\alpha = \frac{u}{w} + \frac{r}{s}\sqrt{d} \in S_n$, com $mdc(u, w) = mdc(r, s) = 1$, então

$$\mathrm{N}(\alpha) = \left(\frac{u}{w}\right)^2 - d\left(\frac{r}{s}\right)^2 = n,$$

e portanto $u^2s^2 - dr^2w^2 = nw^2s^2$. Daqui resulta que $s^2 \mid dr^2w^2$ e que $w^2 \mid u^2s^2$. Como $mdc(r, s) = 1$ e $mdc(u, w) = 1$, tem-se então que $s^2 \mid dw^2$ e que $w^2 \mid s^2$. Uma vez que d é livre de quadrados, segue que $s \mid w$ e $w \mid s$, e portanto $s = w$.

Vejamos agora que se $\alpha \in S_n$ e $v \in \mathbb{Q}[\sqrt{d}]\backslash\{0\}$, então existe no máximo outro ponto α' de S_n tal que $\alpha' = \alpha + tv$, para algum $t \in \mathbb{Q}$. Isto é, observemos que se a recta $\alpha + tv$, que tem declive racional, intersecta o conjunto de pontos de norma n num ponto $\alpha' \neq \alpha$, então este também tem coordenadas racionais. De

$$n = \mathrm{N}(\alpha + tv) = (\alpha + tv)(\overline{\alpha} + \overline{tv}) = \mathrm{N}(\alpha) + t(\alpha\overline{v} + \overline{\alpha}v) + t^2\,\mathrm{N}(v)$$

obtém-se (se $t \neq 0$)

$$0 = t\,\mathrm{N}(v) + (\alpha\overline{v} + \overline{\alpha}v). \tag{3.8}$$

Pondo $\mathrm{tr}(z) = z + \overline{z}$, para $z \in \mathbb{Q}[\sqrt{d}]$, segue então que

$$t = -\frac{\alpha\overline{v} + \overline{\alpha}v}{\mathrm{N}(v)} = -\frac{\mathrm{tr}(\alpha\overline{v})}{\mathrm{N}(v)} \in \mathbb{Q}.$$

Como $\alpha \in S_n$ então $\alpha' = \alpha - \frac{\mathrm{tr}(\alpha\overline{v})}{\mathrm{N}(v)}v \in S_n$. E assim se $\mathrm{tr}(\alpha\overline{v}) \neq 0$, então $\alpha \neq \alpha'$.

Tal como no método de Aubry, o vector v será definido pelo ponto α e pelo ponto δ de $\mathbb{Z}[\sqrt{d}]$ que lhe é mais próximo. Assim vem que $v = \alpha - \delta$ é o vector director da recta $\alpha + tv$ que intersecta a "circunferência" num segundo ponto α'.

Tem-se então

$$\begin{aligned}\alpha' &= \alpha - \frac{\mathrm{tr}(\alpha(\overline{\alpha}-\overline{\delta}))}{\mathrm{N}(\alpha-\delta)}(\alpha-\delta) = \alpha\left(1-\frac{\mathrm{tr}(n-\alpha\overline{\delta})}{\mathrm{N}(\alpha-\delta)}\right)+\frac{\mathrm{tr}(n-\alpha\overline{\delta})}{\mathrm{N}(\alpha-\delta)}\delta \\ &= \frac{1}{\mathrm{N}(\alpha-\delta)}\left[\left(\mathrm{N}(\alpha-\delta)-\mathrm{tr}(n-\alpha\overline{\delta})\right)\alpha+\mathrm{tr}(n-\alpha\overline{\delta})\ \delta\right]\end{aligned}$$

Sabe-se que

$$\mathrm{N}(\alpha-\delta) = (\alpha-\delta)(\overline{\alpha}-\overline{\delta}) = n+\delta\overline{\delta}-(\alpha\overline{\delta}+\overline{\alpha}\delta)$$

e

$$\mathrm{tr}(n-\alpha\overline{\delta}) = n-\alpha\overline{\delta}+n-\overline{\alpha}\delta = 2n-(\alpha\overline{\delta}+\overline{\alpha}\delta) = 2n-\mathrm{tr}(\alpha\overline{\delta}).$$

Pondo $\alpha=\frac{1}{s}\lambda$, com $\lambda\in\mathbb{Z}[\sqrt{d}]$ e $s\in\mathbb{N}$, vem que

$$\frac{\mathrm{tr}(n-\alpha\overline{\delta})}{\mathrm{N}(\alpha-\delta)} = \frac{s\,\mathrm{tr}(n-\alpha\overline{\delta})}{s\,\mathrm{N}(\alpha-\delta)} = \frac{2sn-\mathrm{tr}(\lambda\overline{\delta})}{s\,\mathrm{N}(\alpha-\delta)},$$

tendo-se que

$$s\,\mathrm{N}(\alpha-\delta) = sn-\mathrm{tr}(\lambda\overline{\delta})+s\,\mathrm{N}(\delta)\in\mathbb{N}.$$

Disto tudo resulta que $s\,\mathrm{N}(\alpha-\delta)$ é um múltiplo do denominador de α'. Tem-se que

$$\begin{aligned}\alpha' &= \frac{1}{s\,\mathrm{N}(\alpha-\delta)}\left[\left(s\,\mathrm{N}(\alpha-\delta)-(2sn-\mathrm{tr}(\lambda\overline{\delta}))\right)\alpha+(2sn-\mathrm{tr}(\lambda\overline{\delta}))\ \delta\right] \\ &= \frac{1}{s\,\mathrm{N}(\alpha-\delta)}\left[\left(sn-\mathrm{tr}(\lambda\overline{\delta})+s\,\mathrm{N}(\delta)-(2sn-\mathrm{tr}(\lambda\overline{\delta}))\right)\alpha+(2sn-\mathrm{tr}(\lambda\overline{\delta}))\ \delta\right] \\ &= \frac{1}{s\,\mathrm{N}(\alpha-\delta)}\left[(-n+\mathrm{N}(\delta))\,\lambda+(2sn-\mathrm{tr}(\lambda\overline{\delta}))\ \delta\right],\end{aligned}$$

onde $(-n+\mathrm{N}(\delta))\,\lambda+(2sn-\mathrm{tr}(\lambda\overline{\delta}))\ \delta\in\mathbb{Z}[\sqrt{d}]$.
O denominador de α' é menor que s, pois $\mathrm{N}(\alpha-\delta)<1$. Por conseguinte, a repetição deste processo leva a um elemento de $\mathbb{Z}[\sqrt{d}]$.

Tome-se $d=2$, e seja, por exemplo, $\alpha=\frac{7}{17}+\frac{13}{17}\sqrt{2}$, de norma $\mathrm{N}(\alpha)=1$. O elemento mais próximo de coordenadas inteiras é $\delta=0+1\sqrt{2}$, e assim segue que

$$\mathrm{N}(\alpha-\delta) = \mathrm{N}\left(\frac{7}{17}-\frac{4}{17}\sqrt{2}\right) = \frac{7^2-2\cdot 4^2}{17^2} = \frac{1}{17}\approx 0.059$$

e

$$\mathrm{tr}(n-\alpha\overline{\delta}) = \mathrm{tr}\left(-1-\left(-\frac{26}{17}-\frac{7}{17}\sqrt{2}\right)\right) = \mathrm{tr}\left(\frac{9}{17}+\frac{7}{17}\sqrt{2}\right) = \frac{18}{17}.$$

Portanto

$$\alpha' = \frac{7}{17}+\frac{13}{17}\sqrt{2}-18\left(\frac{7}{17}-\frac{4}{17}\sqrt{2}\right) = -7+5\sqrt{2}$$

é tal que $\mathrm{N}(\alpha')=1$.

Por outro lado, existem formas quadráticas que não são ADC. Por exemplo, usando a forma $g(x, y) = x^2 + dy^2$. Para que g não seja ADC tem de existir pelo menos um $w \in \mathbb{Z}$ tal que $g(x, y) = w$ tenha solução em $\mathbb{Q}^2$, mas não em $\mathbb{Z}^2$. Uma ideia para encontrar uma tal forma é procurar $d, w \in \mathbb{Z}$ tais que a equação $x^2 + dy^2 = w$ não tenha solução inteira, mas tais que exista $n \in \mathbb{N}$ de modo a que $x^2 + dy^2 = n^2 w$ tenha solução inteira.

Observe-se que, como

$$x^2 + dy^2 \equiv w \pmod 4,$$

tem de se ter $w \equiv 0, 1, d, d + 1 \pmod 4$.

Caso $d \equiv 1 \pmod 4$, os números w com $w \not\equiv 3 \pmod 4$ não são pois representados pela forma $x^2 + dy^2$.
Se $d \equiv 2 \pmod 4$, então a congruência não forma qualquer restrição.
Se $d \equiv 3 \pmod 4$, tem-se que $w \not\equiv 2 \pmod 4$ para que a forma acima tenha solução em $\mathbb{Z}^2$.
Por fim, se $d \equiv 0 \pmod 4$, então $w \not\equiv 2, 3 \pmod 4$.

Suponhamos agora que $w \in \mathbb{Z}$ é tal que $g(x, y) = w$ não tem solução em $\mathbb{Z}^2$. Para que $g(x, y) = w$ tenha uma solução em $\mathbb{Q}^2$, tem de existir $n \in \mathbb{N}$ tal que $x^2 + dy^2 = n^2 w$ tenha solução em $\mathbb{Z}^2$. Ora para isso acontecer, n tem que ser par, pois caso contrário teriamos que $w \equiv n^2 w \pmod 4$, e assim $x^2 + dy^2 \not\equiv n^2 w \pmod 4$.

Assim, por exemplo, observando que $5^2 - 17 \cdot 1^2 = 8 = 2 \cdot 2^2$ e que $-17 \equiv 3 \pmod 4$, resulta que a forma $x^2 - 17y^2 = 2$ tem como solução $\left(\frac{5}{2}, \frac{1}{2}\right)$, e que não tem soluções em $\mathbb{Z}^2$. Logo g não é uma forma ADC.

Outro exemplo de uma forma que não é ADC é $g(x, y) = x^2 + 15y^2 = 6$, em que $\left(\frac{3}{2}, \frac{1}{2}\right)$ é uma solução em $(\mathbb{Q} \setminus \mathbb{Z})^2$.

Capítulo 4

Testes Computacionais

Desenvolvemos alguns algoritmos computacionais para estimar o tamanho das classes de Aubry de alguns $\mathcal{Q}_n$. Para tal queremos arranjar uma amostra equidistribuida ou "perfeitamente" aleatória de pontos em $\mathcal{Q}_n$, e verificar a que classes de Aubry cada um desses pontos pertence, estimando assim a medida das classes de Aubry em termos percentuais.
Vamos usar números para os quais conhecemos as suas decomposições como soma de dois quadrados, e usamos o caso mais simples: números que têm só duas decomposições. Temos então que $n = pq$, com p, q primos distintos e $p \equiv q \equiv 1 \pmod 4$, e por isso p e q têm ambos decomposições únicas em soma de dois quadrados: sejam $p = p_1^2 + p_2^2$ e $q = q_1^2 + q_2^2$. Sabe-se pelas equações (2.3) e (2.4) que

$$(p_1q_1 - p_2q_2, p_2q_1 + p_1q_2) \text{ e } (p_1q_1 + p_2q_2, p_2q_1 - p_1q_2)$$

pertencem a $\mathcal{Q}_n \cap \mathbb{Z}^2$, correspondendo às duas decomposições distintas de n em somas de dois quadrados. Portanto, a partir destas decomposições temos oito pontos associados entre si de cada classe de Aubry de $\mathcal{Q}_n$.
Os pontos racionais são gerados à custa de um ponto de partida P de coordenadas inteiras de $\mathcal{Q}_n$, e de um conjunto de rectas de declive racional. Através da proposição 3.4, são consideradas várias rectas de declive racional que passem por P, e que não sejam tangentes a $\mathcal{C}_n$, e registam-se as segundas intersecções de cada recta com a circunferência. De seguida, aplica-se o algoritmo de Aubry a esses pontos racionais para determinar a que classe de Aubry pertencem.

O primeiro algoritmo criado consiste em procurar algum ponto que não pertença à classe de Aubry do ponto de partida P. Considera-se uma recta com um certo declive que passa pelo ponto de partida, e verifica-se se a segunda intersecção não pertence à classe de P. Caso pertença, considera-se outra recta com um declive superior. Repete-se o processo até encontrar algum ponto que pertença à segunda classe de Aubry ou até se iterar o procedimento um número pré-definido de vezes.

Os restantes algoritmos obtêm uma amostra de ponto de $\mathcal{Q}_n$ e retornam a percentagem desses pontos que pertencem à classe de Aubry do ponto de partida. Como os números estudados têm exactamente duas classes de Aubry, os testes contam apenas o número de pontos da amostra que pertencem à classe do ponto de partida, pois os restantes pertencem à outra classe.
O que distingue estes últimos programas é a forma como cada um adquire a amostra de pontos da circunferência. O primeiro algoritmo corresponde a traçar várias rectas de maneira a que a amostra esteja o melhor equidistribuída possível num oitavo de circunferência. Os últimos dois obtêm os pontos da amostra com declives pseudo-aleatórios, em que num é aplicado o algoritmo em $\mathbb{R}^2$ e o outro em $\mathbb{C}$.

Acontece que, para certos números, nenhum algoritmo conseguiu encontrar algum ponto que não pertencesse à classe de Aubry do ponto de partida, independentemente de qual fosse essa classe. Por causa disto, foram utilizados dois pontos de classes de Aubry distintas como pontos iniciais em todos os testes, comparando assim os resultados obtidos.
Portanto, para cada $\mathcal{Q}_n$ registaram-se duas percentagens, cada uma correspondente à classe de Aubry de cada um dos pontos testados. Como qualquer n testado tem exactamente duas classes, a soma dessas percentagens deveria ser aproximadamente 100%. Porém, em alguns casos a soma das percentagens superou largamente esse valor, e em certos casos chegou a atingir os 200%. Aliás, verificou-se que quanto maior fosse n, maior seria a soma das percentagens (até atingir o máximo de 200%). Portanto nenhum destes algoritmos consegue estimar convenientemente as classes de Aubry para qualquer $\mathcal{Q}_n$. Por outro lado, como os algoritmos quase só encontravam pontos da classe de Aubry de n do ponto de partida para os casos em que n tem pelo menos oito algarismos, os resultados obtidos dão a ideia de que as classes dos pontos obtidos dependem da escolha do ponto de partida utilizado nos algoritmos.

Além de estimar as medidas das classes de Aubry, estes algoritmos têm a possibilidade, ainda que remota, de determinar se certos números são compostos e encontrar uma factorização. Se se conhecer uma decomposição de um número qualquer em soma de dois quadrados, e se algum dos algoritmos desenvolvidos encontrar, pelo menos, um ponto que não pertença à classe de Aubry do ponto correspondente a essa decomposição, então pelo teorema 2.28 esse número é composto e pode-se determinar explicitamente uma sua factorização.

4.1 Funções em comum nos algoritmos

O programa utilizado no desenvolvimento dos algoritmos foi o *Pari/GP* [6].

A primeira função desenvolvida foi *myRatP*, que corresponde a traçar uma reta com declive

$\frac{q}{p} \in \mathbb{Q}$ e que passa pelo ponto $(a, b) \in \mathcal{Q}_{a^2+b^2}$, retornando a segunda intersecção dessa recta com a circunferência $\mathcal{Q}_{a^2+b^2}$, se existir. Caso não exista essa segunda interseção, a função retorna o ponto de partida. Portanto, os inputs são a e b, que correspondem às coordenadas de um ponto de $\mathcal{Q}_{a^2+b^2}$, e p e q, que correspondem às coordenadas racionais de um vector.

```
1 myRatP(a,b,p,q) ={
2       local(r,s);
3       r = a - 2*p*(a*p+b*q)/(p^2+q^2);
4       // primeira coordenada
5       s = b - 2*q*(a*p+b*q)/(p^2+q^2);
6       // segunda coordenada
7       return([r,s]);
8       // retorna o ponto de coordenadas (r,s)
9 }
```

Listing 4.1: Função *myRatP*

Este algoritmo permite obter vários pontos de $\mathcal{Q}_n$ a partir de um ponto de partida que lhe pertence, variando o declive da recta. Isto é importante para obter uma amostra de pontos da circunferência.

Será também usada uma função análoga, mas usando a estrutura complexa do plano. A partir de um ponto z da circunferência, considera-se uma recta cujo vector director é $p+qi$. A função devolve a segunda interseção da recta com a circunferência, ou caso esta não exista, a função devolve o ponto z. Acontece que essa segunda intersecção corresponde a uma rotação aplicada a z. O ponto obtido por essa rotação é dado pela equação

$$z \cdot \frac{-\overline{z}^2(q+pi)^2}{|z|^2(p^2+q^2)} = \frac{-\overline{z}(q+pi)^2}{p^2+q^2}.$$

Assim as entradas da função são o elemento z e o vector director $p+qi$. Note-se que na linha de código, I representa o elemento imaginário i.

```
1 myRatCP(z,p,q) ={
2           return(-conj(z)*(q+p*I)^2/(p^2+q^2))
3 }
```

Listing 4.2: Função *myRatCP*

A próxima função *aubry1* implementa o algoritmo de Aubry, ou seja, para cada $v \in \mathcal{Q}_{||v||^2}$, devolve $\mathcal{A}(v)$. Isto é, tem como input um ponto v de $\mathcal{Q}_{||v||^2}$, retornando um representante de coordenadas inteiras da sua classe de Aubry.

```
aubry1(v)={
    local(a,b,P);
    a=v[1]; b=v[2];
    // v = (a,b)
    while(a!=round(a) || b!=round(b),
    // enquanto (a,b) não tiver coordenadas inteiras, o programa corre
        P=myRatP(a,b,a-round(a),b-round(b));
        // segunda intersecção da recta gerada por
        // (a,b) e ([a],[b]) com a circunferência
        a=P[1]; b=P[2];
        //renomeia (a,b) para iterar o comando myRatP
        );
    return([a,b]);
    // retorna um representante da classe de Aubry de v
}
```

Listing 4.3: Algoritmo de Aubry em $\mathcal{Q}_n$

A função *aubryc1* implementa o algoritmo de Aubry em $\mathbb{Q}[i]$, com o elemento de partida z pertencente a $\mathcal{Q}_{z\bar{z}}$, e que retorna um representante de $\mathbb{Z}[i]$ da sua classe de Aubry $\mathcal{A}(z)$.

```
aubryc1(z)={
    local(a,b,P,i);
    a=round(real(z)); b=round(imag(z)); P=z;
    // define-se o ponto de coordenadas inteiras mais perto de z
    while(real(P)!=round(real(P)) || imag(P)!=round(imag(P)),
        // enquanto a + bi não tiver coordenadas inteiras,
        // o programa corre
        P=(conj(P)*(a+b*I-P))/(conj(P)-a+b*I);
        // aplica-se a função f
        a=round(real(P)); b=round(imag(P));
        //renomeia a e b para iterar f
        );
    return(a+b*I);
}
```

Listing 4.4: Algoritmo de Aubry usando $\mathbb{C}$

A próxima função é o núcleo dos testes desenvolvidos, consistindo numa composição do *myRatP* com *aubry1*. Este algoritmo retorna o resultado de considerar uma recta de declive

racional que passe por um ponto escolhido de partida de $\mathcal{Q}_n$ (um ponto conhecido de coordenadas inteiras), e por fim, caso essa recta intersecte a circunferência num segundo ponto, aplica o algoritmo de Aubry a esse mesmo ponto.
A função *rat1* tem como inputs o ponto $(a, b) \in \mathcal{Q}_n$, com $n = a^2 + b^2$, e as coordenadas de um vector director (p, q). O algoritmo começa por usar a função *myRatP* para obter um ponto de coordenadas racionais de $\mathcal{Q}_n$ para depois aplicar o algoritmo de Aubry a esse ponto, obtendo-se assim um "novo"ponto de coordenadas inteiras.

```
1 rat1(a,b,p,q) ={
2     local(z);
3     z = myRatP(a,b,p,q);
4     // o novo ponto
5     return(aubry1(z));
6     //o algoritmo de Aubry aplicado a z
7 }
```

Listing 4.5: Função *rat1*

A função *ratc1* é análoga à função anterior. Neste caso, o ponto de partida é $z = a + bi$, em vez de (a, b), e o vector inicial é $p + qi$. O algoritmo obtém um ponto de coordenadas racionais de $\mathcal{Q}_n$ através da função *myRatCP*, e no final aplica o algoritmo de Aubry a esse ponto.

```
1 ratc1(z,p,q) ={
2     local(w);
3     w = myRatCP(z,p,q);
4     // o novo ponto
5     return(aubryc1(w));
6     //o algoritmo de Aubry aplicado a w
7 }
```

Listing 4.6: Função *ratc1*

4.2 Testes com Escolha Pré-Definida de Pontos de $\mathcal{Q}_n$

O primeiro teste foi denominado por *alg1* e é um algoritmo que consiste em, a partir de um ponto de partida de $\mathcal{Q}_n$, encontrar algum ponto que não pertença à sua classe de Aubry.

Este teste aplica a função *rat1* num ponto de partida $(a, b) \in \mathcal{Q}_n$ com o vector director $(p, 0)$ e verifica se o novo ponto obtido pertence à classe de (a, b). Caso este pertença, então

vai-se aumentando o declive do vector director até se encontrar um ponto que não pertença à classe de (a, b) ou chegar ao limite de iterações q pré-definido. Em particular, o algoritmo corresponde a considerar inicialmente uma recta que passa por (a, b) com o vector director $(p, t) \in \mathbb{Q}^2$, com $t = 0$. Se intersectar $\mathcal{Q}_n$ num segundo ponto u, verifica se esse ponto pertence à mesma classe que (a, b). Se u pertencer à classe de (a, b), retorna o seu resultado aplicando o algoritmo de Aubry; caso contrário, o algoritmo incrementa 1 ao valor de t, e repete este processo. Ou seja, para cada valor de t, o teste considera uma recta distinta que passa por (a, b) e cujo vector diretor é (p, t). O algoritmo realiza incrementos sucessivos até encontrar algum ponto da classe diferente à de (a, b) ou até t igualar um valor pré-definido $q \in \mathbb{Q}$. O teste retorna um ponto que não pertença à classe de Aubry do ponto de partida, bem como o número de iterações necessárias para este ser encontrado, ou devolve o ponto de partida caso t atinja q. Em todo o teste, p é fixo.
Assim, a função *alg1* tem as mesmas entradas que o algoritmo base *rat1*, isto é, o ponto (a, b) e o vector director (p, q); e tem como objetivo procurar algum ponto de $\mathcal{Q}_n$ que não pertença à classe de Aubry de (a, b).

A figura 4.1 dá uma ideia geométrica do procedimento *alg1*: P é o ponto de partida e P'_t é a interseção da recta que passa em P e tem vector director (p, t). Ou seja, os pontos azuis correspondem aos pontos da amostra, e os pontos vermelhos correspondem à aplicação do algoritmo de Aubry a P'_t.

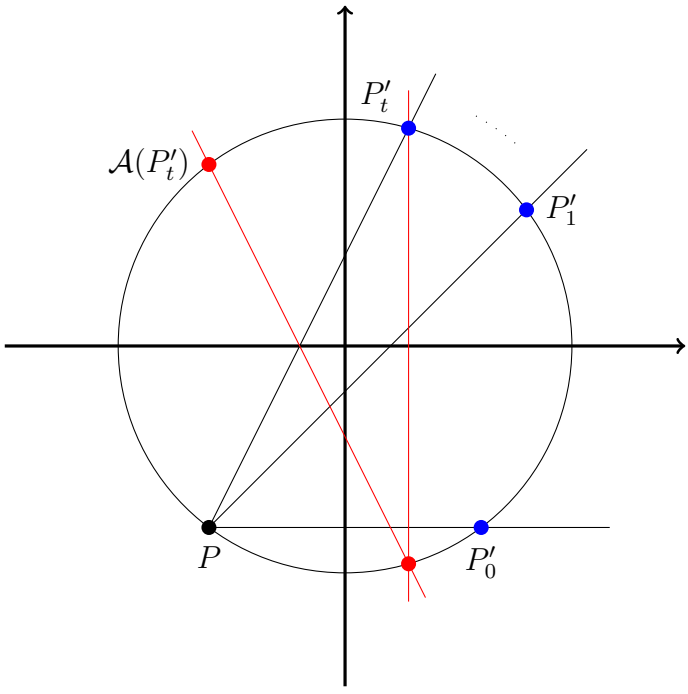

Figura 4.1: Representação Geométrica da Função *alg1*

```
alg1(a,b,p,q)={
    local(t,u);
    t=0;
    while(t<q,
        u=rat1(a,b,p,t)[1];
        // guarda a abcissa do ponto encontrado
        // por rat1 para usar como comparação
        if(
            (u-round(u)==0)
            // se u for inteiro
            && (abs(u)!=abs(a)
            // se u ou -u difere de a
            && abs(u)!=abs(b)),
            // se u ou -u difere de b
            return([rat1(a,b,p,t),t]));
            // retorna um representante da classe de u
            // e retorna t
        t=t+1
        // caso contrário, itera-se t
        );
    return(rat1(a,b,p,q));
}
```

Listing 4.7: Função *alg1*

Fixou-se $q = 10^6$ e testaram-se neste algoritmo os seguintes números:

Exemplo 1:

$$n_1 = 21\ 253 = 142^2 + 33^2 = 138^2 + 47^2 = 401 \cdot 53 = (20^2 + 1^2)(7^2 + 2^2).$$

Repare-se que

$$(20 \cdot 7 + 1 \cdot 2, 20 \cdot 2 - 1 \cdot 7) = (142, 33)$$

e que

$$(20 \cdot 7 - 1 \cdot 2, 20 \cdot 2 + 1 \cdot 7) = (138, 47)$$

pertencem a $\mathcal{Q}_{n_1}$.

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(142, 33)$	$(47, 138)$	10^6	1 763
$(142, 33)$	$(138, -47)$	1	20
$(138, 47)$	$(-142, -33)$	10^6	1 814
$(138, 47)$	$(-33, -142)$	1	23

Tabela 4.1: Resultados – Exemplo 1, *alg1*

Exemplo 2:

$$n_2 = 22\ 601 = 85^2 + 124^2 = 20^2 + 149^2 = 97 \cdot 233 = (4^2 + 9^2)(8^2 + 13^2).$$

$$(149, -20), (-85, 124) \in \mathcal{Q}_{n_2}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(149, -20)$	$(124, -85)$	10^6	1 681
$(149, -20)$	$(85, -124)$	1	22
$(-85, 124)$	$(-20, 149)$	10^6	2 021
$(-85, 124)$	$(20, -149)$	1	54

Tabela 4.2: Resultados – Exemplo 2, *alg1*

Exemplo 3:

$$n_3 = 241\ 001 = 124^2 + 475^2 = 76^2 + 485^2 = 401 \cdot 601 = (20^2 + 1^2)(24^2 + 5^2).$$

$$(485, 76), (475, 124) \in \mathcal{Q}_{n_3}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(485, 76)$	$(-124, 475)$	10^6	526
$(485, 76)$	$(475, -124)$	1	20
$(475, 124)$	$(-485, -76)$	10^6	545
$(475, 124)$	$(-485, 76)$	1	381

Tabela 4.3: Resultados – Exemplo 3, *alg1*

Exemplo 4:

$$n_4 = 88\ 555\ 513 = 9133^2 + 2268^2 = 5997^2 + 7252^2$$
$$= 8009 \cdot 11\ 057 = (85^2 + 28^2)(89^2 + 56^2).$$

$$(9133, 2268), (5997, 7252) \in \mathcal{Q}_{n_4}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(9\ 133, 2\ 268)$	$(7\ 252, -5\ 997)$	10^6	1 632
$(9\ 133, 2\ 268)$	$(-5\ 997, 7\ 252)$	1	3 355
$(5\ 997, 7\ 252)$	$(-9\ 133, 2\ 268)$	10^6	1 985
$(5\ 997, 7\ 252)$	$(2\ 268, -9\ 133)$	1	283

Tabela 4.4: Resultados – Exemplo 4, *alg1*

Exemplo 5:

$$n_5 = 1\ 656\ 747\ 613 = 40\ 562^2 + 3\ 387^2 = 3\ 718^2 + 40\ 533^2$$
$$= 30\ 013 \cdot 55\ 201 = (123^2 + 122^2)(180^2 + 151^2).$$

$$(40\ 562, -3\ 387), (3\ 718, 40\ 533) \in \mathcal{Q}_{n_5}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(40\ 562, -3\ 387)$	$(-40\ 533, -3\ 718)$	10^6	4 076
$(40\ 562, -3\ 387)$	$(-3\ 718, -40\ 533)$	1	22 674
$(3\ 718, 40\ 533)$	$(40\ 562, 3387)$	10^6	3 881
$(3\ 718, 40\ 533)$	$(3\ 387, -40\ 562)$	1	245

Tabela 4.5: Resultados – Exemplo 5, *alg1*

Exemplo 6:

$$n_6 = 25\ 926\ 311\ 852\ 773$$
$$= 4\ 915\ 263^2 + 1\ 329\ 098^2 = 4\ 704\ 897^2 + 1\ 946\ 858^2$$
$$= 7\ 777\ 801 \cdot 3\ 333\ 373 = (2\ 640^2 + 899^2)(1\ 822^2 + 117^2).$$

$$(4\ 915\ 263, -1\ 329\ 098), (4\ 704\ 897, 1\ 946\ 858) \in \mathcal{Q}_{n_6}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(4\ 915\ 263, -1\ 329\ 098)$	$(-4\ 704\ 897, -1\ 946\ 858)$	10^6	570 405
$(4\ 915\ 263, -1\ 329\ 098)$	$(1\ 946\ 858, -4\ 704\ 897)$	1	199 417
$(4\ 704\ 897, 1\ 946\ 858)$	$(1\ 329\ 098, -4\ 915\ 263)$	10^6	42 144
$(4\ 704\ 897, 1\ 946\ 858)$	$(-1\ 329\ 098, 4\ 915\ 263)$	1	50 461

Tabela 4.6: Resultados – Exemplo 6, *alg1*

Exemplo 7:

$$\begin{aligned} n_7 &= 56\ 311\ 388\ 274\ 131\ 521 \\ &= 237\ 120\ 161^2 + 9\ 242\ 160^2 = 223\ 243\ 911^2 + 80\ 458\ 340^2 \\ &= 123\ 456\ 461 \cdot 456\ 123\ 461 = (10\ 906^2 + 2\ 125^2)(21\ 106^2 + 3\ 265^2). \end{aligned}$$

$$(237\ 120\ 161, -9\ 242\ 160), (223\ 243\ 911, 80\ 458\ 340) \in \mathcal{Q}_{n_7}.$$

Ponto de Partida (a, b)	Ponto Final	p	Iterações
$(237\ 120\ 161, -9\ 242\ 160)$	$(9\ 242\ 160, -237\ 120\ 161)$	10^6	10^6
$(237\ 120\ 161, -9\ 242\ 160$	$(-237\ 120\ 161, -9\ 242\ 160$	1	10^6
$(223\ 243\ 911, 80\ 458\ 340)$	$(-80\ 458\ 340, -223\ 243\ 911)$	10^6	10^6
$(223\ 243\ 911, 80\ 458\ 340)$	$(-223\ 243\ 911, -80\ 458\ 340)$	1	10^6

Tabela 4.7: Resultados – Exemplo 7, *alg1*

Pelos resultados obtidos, e observando o número de iterações que a função *alg1* necessitou até terminar, vê-se que existem classes mais fáceis de encontrar que outras. Aliás, no último exemplo é impossível descobrir a outra classe distinta à qual o ponto de partida não pertence. Como a partir de certos números era impossível encontrar qualquer ponto que não pertencesse à classe de Aubry de qualquer ponto de partida, a motivação nos algoritmos seguintes foi estimar a medida dessas classes de Aubry.

No próximo teste, a escolha de pontos para a amostra de $\mathcal{Q}_n$ baseia-se em considerar n rectas definidas por um ponto de partida fixo e que passam por pontos de coordenadas racionais próximos da circunferência, tais que essas rectas dividam o oitavo de circunferênca $\mathcal{Q}_n/\sim$

(ver secção 3.2), em $n-1$ arcos aproximadamente idênticos. Desta maneira consegue-se uma amostra distribuída espalhada pelo oitavo de circunferência. Esses pontos próximos da circunferência obtêm-se truncando as coordenadas de pontos de $\mathcal{Q}_n$ a partir de uma certa casa decimal.
Observe-se que essas rectas não dividem perfeitamente $\mathcal{Q}_n/\sim$, pois para esse efeito deveriam ter declive irracional e assim não era garantido que essas rectas intersectassem $\mathcal{Q}_n$.
Por fim, aplica-se o algoritmo de Aubry aos pontos obtidos de $\mathcal{Q}_n$ através dessas rectas, contam-se os que pertencem à classe do ponto do input da função, e o teste retorna a percentagem de pontos que pertence à classe de Aubry do ponto de partida. Esperava-se que este algoritmo desse uma estimativa da medida das classes de Aubry da circunferência.

O teste é designado por *prob2*, e tem como entradas o ponto de partida $v = (v_1, v_2) \in \mathcal{Q}_n$, o número de rectas m e o número de casas decimais pr escolhidas para truncar os valores das coordenadas dos pontos racionais próximos da circunferência.
Inicialmente tem-se $w = (-|v_1|, |v_2|)$, um associado de v que pertença ao 2^o quadrante. As coordenadas dos pontos da circunferência são da forma $(\sqrt{n}\cos\theta, \sqrt{n}\sin\theta)$, com $\theta \in [0, 2\pi[$, e como existe um grande risco destas serem irracionais, trunca-se o valor na casa decimal pr. Isto também evita que as rectas sejam tangentes a $\mathcal{Q}_n$, já que estes pontos encontram-se dentro da circunferência. De seguida, *rep* é um representante de coordenadas inteiras da classe de Aubry de v, e é utilizado para verificar se os pontos da amostra pertencem à sua classe.
Depois têm-se as iterações da função, que correspondem a traçar m rectas que passam por w e pelos pontos pontos racionais próximos da circunferência. Os ângulos formados por estes últimos com o semi-eixo positivo das abcissas são aproximadamente da forma $\frac{k\pi}{4m}$, com $k \in \{0, ..., m-1\}$. Assim as rectas vão intersectando $\mathcal{Q}_n/\sim$ desde um ponto próximo dos zero radianos até um ponto próximo dos $\pi/4$ radianos, de modo a que os arcos formados por interseções sucessivas tenham medidas mais ou menos idênticas.
Por fim, o programa retorna a percentagem de pontos da amostra obtida que pertence à classe do ponto de partida.

A figura 4.2 ilustra a ideia subjacente à função *prob2*: V é o ponto de partida, W é um associado de V no 2^o quadrante e W_i', com $i \in \{0, ..., m-1\}$, são as segundas interseções obtidas pelas rectas, ou seja, os pontos da amostra.

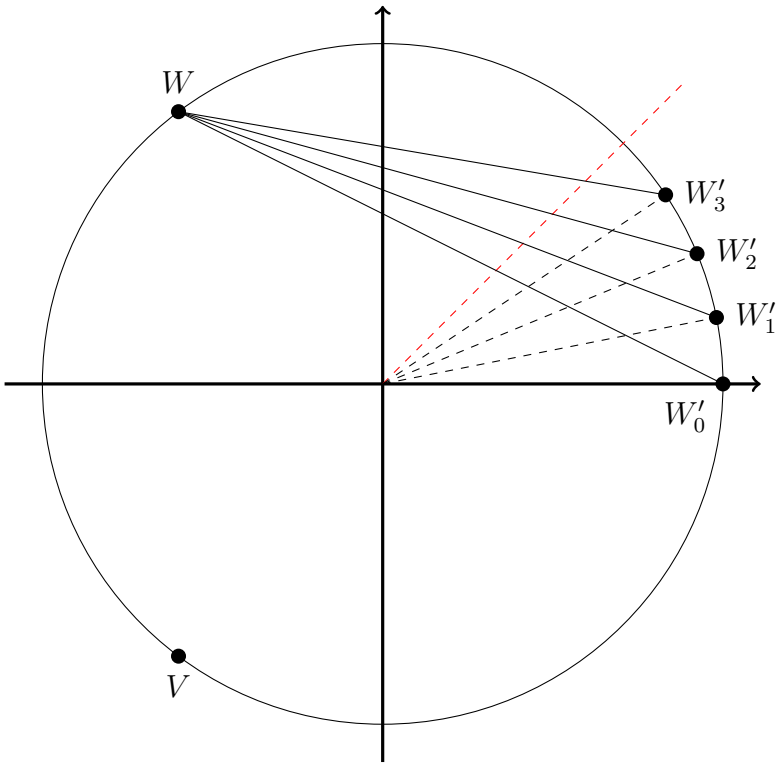

Figura 4.2: Representação Geométrica da Função *prob2*

```
prob2(v,m,pr)={
    gettime();
    local(w,p,rep,i,j,u,N);
    i=0; j=0;
    w=[-abs(v[1]),abs(v[2])];
    // w pertence ao segundo quadrante
    p=aubry1(v);
    rep=[abs(p[1]),abs(p[2])];
    // representante da classe de v
    N=v[1]^2+v[2]^2;
    while(i<m,
        u=rat1(
        w[1],w[2],
        floor((10^pr)*sqrt(N)*cos((i*Pi)/(4*m)))*10^(-pr)-w[1],
        floor((10^pr)*sqrt(N)*sin((i*Pi)/(4*m)))*10^(-pr)-w[2]
        );
        if((abs(u[1])==rep[1] || abs(u[2])==rep[1]),j=j+1);
        // j aumenta 1 valor se u pertence a classe de v
        i=i+1
```

```
20          // itera-se na recta que intersecta a circunferência
21          );
22      t=gettime();
23      // t mede o tempo de execução
24      print(t);
25      return(j/m);
26  }
```

Listing 4.8: Função prob2

Para os números utilizados no algoritmo anterior, obteve-se os seguintes resultados com $m = 10^5$ iterações e $pr = 50$.

Exemplo 1:
$n_1 = 21\ 253$

Ponto de Partida	% aproximada	Tempo (s)
$(142, 33)$	49,1	268, 685
$(138, 47)$	49,0	255, 074

Tabela 4.8: Resultados – Exemplo 1, *prob2*

Exemplo 2:
$n_2 = 22\ 601$

Ponto de Partida	% aproximada	Tempo (s)
$(149, -20)$	46,0	362, 029
$(-85, 124)$	56,4	363, 562

Tabela 4.9: Resultados – Exemplo 2, *prob2*

Exemplo 3:
$n_3 = 241\ 001$

Ponto de Partida	% aproximada	Tempo (s)
$(485, 76)$	82,9	340, 179
$(475, 124)$	83,2	342, 199

Tabela 4.10: Resultados – Exemplo 3, *prob2*

Exemplo 4:
$n_4 = 88\ 555\ 513$

Ponto de Partida	% aproximada	Tempo (s)
$(9\ 133, 2\ 268)$	98,5	399, 593
$(5\ 997, 7\ 252)$	98,7	392, 111

Tabela 4.11: Resultados – Exemplo 4, *prob2*

Exemplo 5:
$n_5 = 1\ 656\ 747\ 613$

Ponto de Partida	% aproximada	Tempo (s)
$(40\ 562, -3\ 387)$	99,8	402, 618
$(3\ 718, 40\ 533)$	99,8	398, 843

Tabela 4.12: Resultados – Exemplo 5, *prob2*

Exemplo 6:
$n_6 = 25\ 926\ 311\ 852\ 773$

Ponto de Partida	% aproximada	Tempo (s)
$(4\ 915\ 263, -1\ 329\ 098)$	99,9	433, 157
$(4\ 704\ 897, 1\ 946\ 858)$	99,9	430, 832

Tabela 4.13: Resultados – Exemplo 6, *prob2*

Exemplo 7:
$n_7 = 56\ 311\ 388\ 274\ 131\ 521$

Ponto de Partida	% aproximada	Tempo (s)
$(237\ 120\ 161, -9\ 242\ 160)$	100	465, 664
$(223\ 243\ 911, 80\ 458\ 340)$	100	481, 813

Tabela 4.14: Resultados – Exemplo 7, *prob2*

Verifica-se que, em geral, a soma das percentagens obtidas para cada exemplo não está sequer próximo de 100%, e por isso o algoritmo não é fiável para estimar as medidas das classes de Aubry. Observa-se ainda que quanto maior o número, maior é a tendência da função não encontrar qualquer ponto que não pertença à classe do ponto de partida.

4.3 Escolha Aleatória de Pontos da Circunferência

Para os restantes algoritmos, mudou-se o método de se obter as amostras de pontos de $\mathcal{Q}_n$. Pelo facto dos pontos no teste anterior serem escolhidos de uma maneira pré-definida poderia causar alguma influência na aplicação do algoritmo de Aubry nos pontos da amostra, e por isso utilizou-se um método aleatório para se obter amostras de pontos de $\mathcal{Q}_n$.

Uma distribuição uniforme de pontos na circunferência unitária pode ser obtida escolhendo um número real aleatório entre 0 e 2π, correspondendo ao ângulo que o ponto faz com o semi-eixo positivo das abcissas. Nos seguintes testes utiliza-se outro método que nós denominaremos por *Escolha Aleatória de Pontos da Circunferência*. Neste método, como é mostrado em [8], os pontos escolhidos aleatoriamente na circunferência são obtidos tomando dois números x_1 e x_2 de uma distribuição uniforme em $[-1, 1]$, rejeitando os pares com $x_1^2 + x_2^2 \geq 1$.

Aplicando as fórmulas do dobro do ângulo da trigonometria nos pares de valores (x_1, x_2) gerados, em que x_1 e x_2 correspondem a $\cos(2\alpha)$ e $\sin(2\alpha)$ respectivamente, para algum $\alpha \in [0, 2\pi]$, obtêm-se pontos da circunferência unitária da forma

$$x = \frac{2x_1x_2}{x_1^2 + x_2^2} \tag{4.1}$$

e

$$y = \frac{x_1^2 - x_2^2}{x_1^2 + x_2^2}. \tag{4.2}$$

Desta maneira tem-se uma escolha aleatória de pontos da circunferência unitária a partir de uma distribuição uniforme. A partir dos pontos desta circunferência, é possível obter pontos próximos de $\mathcal{Q}_n$, multiplicando as coordenadas por um valor racional próximo de $\sqrt{n}$. Se a circunferência pertencer a $\mathbb{C}$, basta multiplicar os valores $x_1 + x_2 i$ gerados por quaisquer pontos de $\mathcal{Q}_n$ para se obter amostras.

4.4 Testes com Escolha Aleatória de Pontos de $\mathcal{Q}_n$

No algoritmo seguinte, a obtenção da amostra corresponde a traçar rectas, a partir de um ponto de partida fixo, que intersectem pontos de $\mathcal{Q}_n$, de forma pseudo-aleatória e uniformemente distribuída, e que estejam próximos de $\mathcal{Q}_n$. Estes últimos são obtidos pela Escolha Aleatória de Pontos da Circunferência (acima descrito), e multiplica-se cada um destes por um número que corresponde à truncatura de $\sqrt{n}$. Assim, cada uma das rectas vai intersectar a circunferência num segundo ponto, obtendo-se assim a amostra desejada. Por fim, aplica-se o algoritmo de Aubry nos pontos da amostra e o teste retorna a percentagem desses pontos que pertence à classe de Aubry do ponto de partida.

O teste é designado por *prob4*, e tem como inputs o ponto de partida $v \in \mathcal{Q}_n$, o número de rectas m, o limite superior r da função $random()$, utilizado para obter os valores da distribuição uniforme na Escolha Aleatória de Pontos da Circunferência, e o tamanho tr da truncatura de $\sqrt{n}$, garantido que o número obtido é racional.
Tal como o teste anterior, define-se w como um associado de v pertencente ao 2^o quadrante e toma-se rep como um representante de coordenadas inteiras da classe de Aubry de v. Tem-se que N é o quadrado do raio da circunferência e que M é uma aproximação de N, com tr a ser a casa decimal em que o valor é truncado, precavendo o caso de N ser irracional. Utiliza-se a Escolha Aleatória de Pontos da Circunferência para se obter pontos da circunferência unitária. Primeiro tomam-se pares de valores, neste caso da distribuição uniforme $[0, 1]$, que vão gerar no fim pontos cujas coordenadas se obtêm das equações (4.1) e (4.2). Note-se que os pontos obtidos encontram-se na semicircunferência em que as abcissas são sempre positivas.

A existência do associado de v e o facto de apenas se obterem pontos da semicircunferência com a primeira coordenada positiva têm como objetivo evitar que as rectas obtidas sejam tangentes ao ponto de partida devido aos arredondamentos do computador.
Multiplicam-se estes últimos por M, dando origem a pontos racionais próximos de $\mathcal{Q}_n$. Consideram-se as rectas que passam pelo ponto de partida e pelos pontos próximos da circunferência obtidos. Estas rectas vão intersectar novos pontos na circunferência de raio $\sqrt{n}$, obtendo-se assim a amostra, e de seguida aplica-se o algoritmo de Aubry nesses pontos. No fim, o algoritmo retorna a percentagens de pontos da amostra que pertencem à classe de Aubry do ponto de partida v.

A figura 4.3 ilustra a ideia subjacente à função *prob4*: V é o ponto de partida, W é um associado de V no 2^o quadrante e W'_i, com $i \in \{0, ..., 3\}$, são os pontos da amostra obtida.

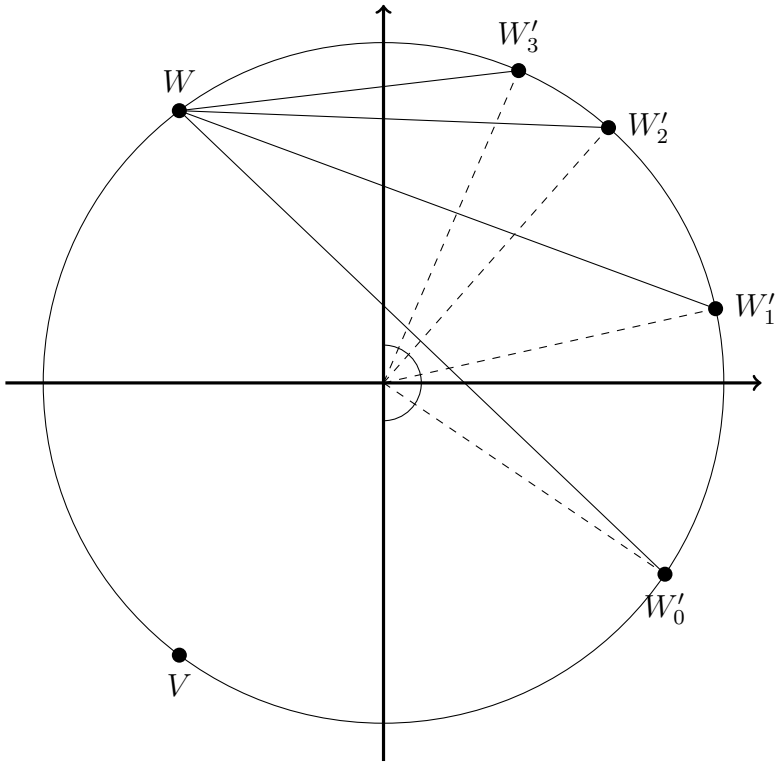

Figura 4.3: Representação Geométrica da Função *prob4*

```
1  prob4(v, m, r, tr) ={
2      gettime();
3      local(w, p, rep, i, j, a, b, a1, b1, u, N, M, t);
4      i = 0;  j = 0;  a = 1;  b = 1;
5      w = [-abs(v[1]),abs(v[2])];
6      p = aubry1(v);
7      rep = [abs(p[1]),abs(p[2])];
```

```
8       // representante da classe de v
9       N = v[1]^2 + v[2]^2;
10      M =floor((10^tr)*sqrt(N))/(10^tr);
11      // raio aproximado da circunferência
12      while(i < m,
13            while(a^2 + b^2 >= 1,
14                  a = (random(r) + 1)/r;  b = (random(r) + 1)/r);
15            a1 = (2 * a * b)/(a^2 + b^2); b1 = (a^2 - b^2)/(a^2 + b^2);
16            // Escolha Aleatória de Pontos da Circunferência
17            u = rat1(w[1], w[2], M * a1 - w[1], M * b1 - w[2]);
18            // vector director (M*(a1,a2) - w)
19            if((abs(u[1]) == rep[1] || abs(u[2]) == rep[1]), j = j + 1);
20            // Verificar a classe de u
21            i = i + 1;  a = 1;  b = 1;
22            );
23      t=gettime();
24     // t mede o tempo de execução
25      print(t);
26      return(j/m);
27  }
```

Listing 4.9: prob4

Para os números utilizados no algoritmo anterior, obteve-se os seguintes resultados com $m = 10^5$ iterações, $tr = 50$ e $r = 100$.

Exemplo 1:
$n_1 = 21\ 253$

Ponto de Partida	% aproximada	Tempo (s)
$(142, 33)$	49,3	243, 800
$(138, 47)$	54,3	245, 659

Tabela 4.15: Resultados – Exemplo 1, *prob4*

Exemplo 2:
$n_2 = 22\ 601$

Ponto de Partida	% aproximada	Tempo (s)
$(149, -20)$	43,2	245, 790
$(-85, 124)$	58,6	246, 118

Tabela 4.16: Resultados – Exemplo 2, *prob4*

Exemplo 3:
$n_3 = 241\ 001$

Ponto de Partida	% aproximada	Tempo (s)
$(485, 76)$	82,6	344, 153
$(475, 124)$	84,4	344, 539

Tabela 4.17: Resultados – Exemplo 3, *prob4*

Exemplo 4:
$n_4 = 88\ 555\ 513$

Ponto de Partida	% aproximada	Tempo (s)
$(9\ 133, 2\ 268)$	98,6	395, 821
$(5\ 997, 7\ 252)$	99,0	393, 788

Tabela 4.18: Resultados – Exemplo 4, *prob4*

Exemplo 5:
$n_5 = 1\ 656\ 747\ 613$

Ponto de Partida	% aproximada	Tempo (s)
$(40\ 562, -3\ 387)$	99,8	413, 714
$(3\ 718, 40\ 533)$	99,8	415, 499

Tabela 4.19: Resultados – Exemplo 5, *prob4*

Exemplo 6:
$n_6 = 25\ 926\ 311\ 852\ 773$

Ponto de Partida	% aproximada	Tempo (s)
$(4\ 915\ 263, -1\ 329\ 098)$	100	448, 503
$(4\ 704\ 897, 1\ 946\ 858)$	99,9	458, 048

Tabela 4.20: Resultados – Exemplo 6, *prob4*

Exemplo 7:
$n_7 = 56\ 311\ 388\ 274\ 131\ 521$

Ponto de Partida	% aproximada	Tempo (s)
$(237\ 120\ 161, -9\ 242\ 160)$	100	451, 567
$(223\ 243\ 911, 80\ 458\ 340)$	100	447, 301

Tabela 4.21: Resultados – Exemplo 7, *prob4*

Os resultados gerais obtidos com este programa não variaram muito em relação ao algoritmo computacional anterior, e portanto não é um teste fiável para estimar as medidas das classes de Aubry. Apesar disso, este algoritmo tem um tempo de execução ligeiramente menor na maioria dos números testados.

O próximo teste foi realizado em $\mathbb{C}$ e também utilizou a Escolha Aleatória de Pontos da Circunferência para obter uma amostra de pontos. A ideia desta abordagem era diminuir o tempo de execução dos algoritmos anteriores, substituindo o processo de obter rectas e registar as segundas intersecções por rotações em $\mathbb{C}$. Em particular, ao invés de se gerarem pontos pseudo-aleatórios próximos da circunferência, multiplicam-se directamente os pontos

da circunferência unitária pelo ponto de partida, aplicando-lhe assim uma rotação centrada na origem.

O algoritmo tem o ponto de partida, e realiza produtos sucessivos com pontos da circunferência unitária, verificando sempre se os pontos obtidos pertencem à classe de Aubry do ponto de partida. No final, retorna a percentagem de pontos que estão nessa classe.

O teste designa-se por *probc2* e os seus inputs são o ponto de partida z, o número m de rotações realizadas e o limite superior r da função $random()$, utilizado para obter os valores da distribuição uniforme na Escolha Aleatória de Pontos da Circunferência. Neste teste, a distribuição uniforme utilizada é $[-1, 1]$.
O algoritmo obtém os pontos u_i, com $i \in \{0, m-1\}$, da circunferência unitária pela Escolha Aleatória de Pontos da Circunferência, aplica-se o algoritmo de Aubry nos pontos

$$z_i = z \prod_{i=0}^{m-1} u_i$$

e por fim retorna a percentagem desses pontos que pertencem à classe de Aubry do ponto de partida z.

A figura 4.4 ilustra a ideia subjacente à função *probc2*: z é o ponto de partida, u_i são os pontos da circunferência unitária gerados pela Escolha Aleatória de Pontos da Circunferência, com $i \in \{1, 2, 3\}$, e $z_i = z \prod_{i=1}^{3} u_i$ são os pontos da amostra.

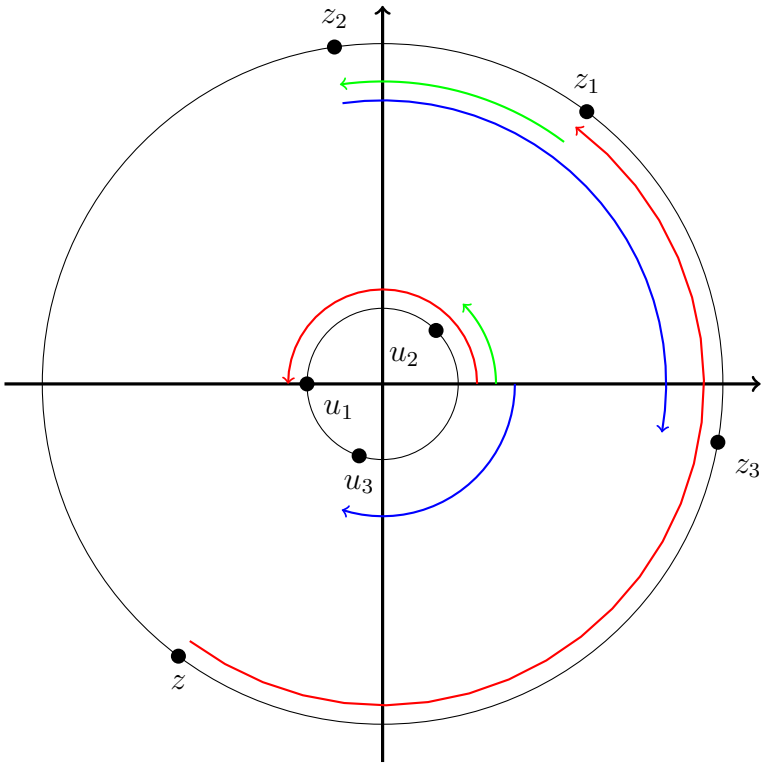

Figura 4.4: Representação Geométrica da Função *probc2*

```
probc2(z, m, r) ={
    gettime();
    local(p, rep, l, j, u, a, b, a1, b1);
    l = 0;  j = 0;  a = 1;  b = 1;
    p = aubryc1(z);
    rep =abs(real(p))+abs(imag(p)) * I;
    // representante da classe
    while(l < m,
        while(a^2 + b^2 >= 1 || a^2 + b^2 == 0,
            a = (random(2 * r - 1) + 1 - r)/r;
            b = (random(2 * r - 1) + 1 - r)/r);
        a1 = (a^2 - b^2)/(a^2 + b^2);  b1 = (2 * a * b)/(a^2 + b^2);
        // elemento obtido pela EAPC
        u = z * (a1 + b1 * I);
        // u é o novo ponto da amostra
        if(
            abs(real(aubryc1(u))) == real(rep)
            || abs(imag(aubryc1(u))) == real(rep),
            j = j + 1);
```

```
20            // comparam-se as classes de z e u
21            z = u;
22            l = l + 1;  a = 1;  b = 1;
23            );
24        t=gettime();
25        // t mede o tempo de execução
26        print(t);
27        return(j/m);
28    }
```

Listing 4.10: Teste de Aubry em $\mathbb{C}$

Para os números utilizados no algoritmo anterior, obteve-se os seguintes resultados com $m = 10^3$ iterações e com o limite superior $r = 50$.

Exemplo 1:
$n_1 = 21\ 253$

Ponto de Partida	% aproximada	Tempo (s)
$142 + 33i$	49,0	43, 340
$138 + 47i$	52,1	38, 484

Tabela 4.22: Resultados – Exemplo 1, *probc2*

Exemplo 2:
$n_2 = 22601$

Ponto de Partida	% aproximada	Tempo (s)
$149 - 20i$	42,8	44, 574
$-85 + 124i$	58,0	45, 280

Tabela 4.23: Resultados – Exemplo 2, *probc2*

Exemplo 3:
$n_3 = 241\ 001$

Ponto de Partida	% aproximada	Tempo (s)
$485 + 76i$	52,5	90, 971
$475 + 124i$	50,5	124, 510

Tabela 4.24: Resultados – Exemplo 3, *probc2*

Exemplo 4:
$n_4 = 88\ 555\ 513$

Ponto de Partida	% aproximada	Tempo (s)
$9\ 133 + 2\ 268i$	94,7	157, 279
$5\ 997 + 7\ 252i$	96,8	98, 254

Tabela 4.25: Resultados – Exemplo 4, *probc2*

Exemplo 5:
$n_5 = 1\ 656\ 747\ 613$

Ponto de Partida	% aproximada	Tempo (s)
$40\ 562 - 3\ 387i$	99,1	117, 740
$3\ 718 + 40\ 533i$	99,4	150, 894

Tabela 4.26: Resultados – Exemplo 5, *probc2*

Exemplo 6:
$n_6 = 25\ 926\ 311\ 852\ 773$

Ponto de Partida	% aproximada	Tempo (s)
$4\ 915\ 263 - 1\ 329\ 098i$	99,9	18, 271
$4\ 915\ 263 - 1\ 329\ 098i$	100	126, 984
$4\ 704\ 897 + 1\ 946\ 858i$	100	149, 695

Tabela 4.27: Resultados – Exemplo 6, *probc2*

Exemplo 7:
$n_7 = 56\ 311\ 388\ 274\ 131\ 521$

Ponto de Partida	% aproximada	Tempo (s)
$237\ 120\ 161 - 9\ 242\ 160i$	100	159, 672
$223\ 243\ 911 + 80\ 458\ 340i$	100	153, 576

Tabela 4.28: Resultados – Exemplo 7, *probc2*

Neste algoritmo apenas se verificou uma mudança significativa no exemplo 3, no qual se aproximou de percentagens mais aceitáveis, enquanto que nos restantes casos os valores alteraram pouco em comparação com os testes anteriores. Ao contrário do que se esperava, o tempo de execução foi bem superior aos algoritmos anteriores, daí o número de iterações utlizados nos exemplos ter sido menor.

O exemplo 6 tem dois resultados para o ponto de partida $4\ 915\ 263 - 1\ 329\ 098i$, pois o teste só encontrou pontos que não pertenciam à classe de Aubry do ponto de partida uma vez. O teste não encontrou algum desses pontos noutras tentativas.

Observando os resultados obtidos pelos últimos três algoritmos, conclui-se que nenhum é fiável para estimar a medida das classes de Aubry. Especialmente por existirem números em que nenhum dos testes consegue detectar a classe à qual o ponto de partida não pertence. Aparentemente, quanto maior for n, maior é a tendência dos resultados nos três testes serem 100%, independentemente da escolha do ponto de partida.

Capítulo 5

Conclusão

Os números da forma $n = pq$, tais que p e q são primos distintos da forma $4k + 1$, com $k \in \mathbb{Z}$, têm exactamente duas decomposições distintas como soma de dois quadrados.
Dois pontos racionais da circunferência $\mathcal{Q}_n$ pertencem à mesma classe de Aubry se estes retornarem elementos associados entre si (no sentido da definição da página 24), ao lhes aplicar o algoritmo de Aubry. Portanto, as circunferências consideradas têm exactamente duas classes de Aubry.

Foram criados algoritmos para obter amostras de pontos racionais de circunferências a partir de um ponto de partida. Posteriormente, verificou-se se existia algum ponto que não pertencesse à classe de Aubry do ponto que gerou a amostra ou mostraram-se as percentagens de pontos das amostras que pertenciam à classe de Aubry do ponto de partida. Acontece que quanto maior for n, mais dificuldade os algoritmos tiveram em encontrar pontos que não pertencessem à classe de Aubry do ponto de partida. Aliás, a certa altura, nenhum algoritmo encontrou a segunda classe.

Apesar das classes de Aubry serem mensuráveis, com os algoritmos desenvolvidos neste trabalho foi impossível estimar as suas medidas em geral. Por outro lado, os resultados obtidos são misteriosos, e podem ser fonte de estudo no futuro.
A única garantia é que se algum destes testes encontrar duas classes de algum $\mathcal{Q}_n$, então n é seguramente composto, e pode-se explicitar uma factorização sua.

Para trabalhos futuros, seria interessante encontrar uma maneira diferente de se obter uma amostra de pontos de $\mathcal{Q}_n$ para verificar se existiriam alterações nos resultados aplicando o algoritmo de Aubry.
Outro trabalho possível seria utilizar outras formas quadráticas, que não a equação da circunferência, e relacionar eventuais resultados com a possibilidade de se fatorizarem certos números. Por exemplo, se existirem duas soluções naturais distintas em $x^2 + 2y^2 = n$, verificar se é possível obter decomposições de alguns números compostos da forma $4k + 3$.

Bibliografia

[1] Patrick Billingsley. *Probability and Measure*. John Wiley & Sons Inc., 3 edition, 1995.

[2] David M. Burton. *Elementary Number Theory*. McGraw-Hill, 2002.

[3] John B. Fraleigh. *A First Course in Abstract Algebra*. Pearson Education Limited, 7 edition, 2014.

[4] William J. LeVeque. *Fundamentals of Number Theory*. Dover Publications, 1996.

[5] Øystein Ore. *Number Theory and Its History*. McGraw-Hill, 1988.

[6] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`.

[7] André Weil. *Number Theory: An approach through history*. Birkhäuser, 1987.

[8] Eric W. Weisstein. "Circle Point Picking". *MathWorld – A Wolfram Web Resource*. `http://mathworld.wolfram.com/CirclePointPicking.html`.